

Partial Translation of Reference 1

Jpn. Pat. Appln. KOKAI Publication No. 2002-055959

Filing No.: 2000-243787

Filing Date: August 11, 2000

Applicant: MACKPORT BIO-SECURITY CORP

Priority: Not Claimed

KOKAI Date: February 20, 2002

Request for Examination: Not filed

Int.Cl.: G06F 15/00

17/60

G09C 1/00

H04L 9/32

[A]

Column 14, Line 25 to Line 37

[0047] Further, in addition to the above aspect of the invention, according to another aspect of the invention, the information terminal includes a living body information registering means that registers living body information of a specific person for matching, a passport information storing means that stores passport information corresponding to the living body information registered in the living body information registering means, a living body information matching means for matching the living body information, in which a characteristic point is extracted by the characteristic point extracting means from the living body information read by the living body information reading means, with the living body information registered for matching in the living body information registering means, and an accessing means for taking out corresponding passport information from the passport information storing means and accessing a service site corresponding to the passport information when both pieces of the living body information match with each other as a result of the matching by the living body information matching means.

[B]

Column 19, Line 48 to Column 20, Line 27

[0080] A first one of the three patterns of configurations has a client terminal authentication type configuration as shown in FIG. 1. In this configuration, authentication is carried out in the inside of the client terminal 11 so an Internet passport is obtained. In a configuration of the memory area 16 of the client terminal authentication type, a living body information characteristic point data 20, such as fingerprint characteristic point data, exists in the RAM 17. Also, an Internet passport area 21 and a work area 22 exist together with the living body information characteristic point data 20. Among them, the Internet passport area 21 plays a role as the passport information storing means, and is not destroyed even when power is cut off.

[0081] In addition, the ROM 18 stores operation software 23, a characteristic point extraction algorithm 24, a living body information matching algorithm 25, and a key information storage section 26 that stores a secret key PC-B and a public key SS-A. Further, the living body information characteristic point data 20 registers living body information of a specific person for matching, and has a function as the living body

information registering means.

[0082] Among them, the operation software 23 is read first in the CPU 15 when the information terminal is turned on. The operation software 23 includes a high-order application and a low-order application.

[0083] In addition, the ROM 18 also stores the characteristic point extraction algorithm 24 as the characteristic point extracting means. The characteristic point extraction algorithm 24 extracts a characteristic point from living body information read by the living body information reading means 12. Then, the extracted characteristic point of the living body information is stored in the RAM 17 for matching in advance.

[C]

Column 22, Line 43 to Column 23, Line 22

[0098] In this state, the user accesses the specific service site 40 by using the client terminal 11 as shown in FIG. 4. Then, if the user desires to purchase a product, and view and download an information content in the service site 40. Then, the service site 40 side requests authentication with respect to the user, since there is the need for user authentication. In this case, for example, a Web screen of the service site 40 displays an "authentication button" and the like, and the user clicks the authentication button.

[0099] When the user clicks the authentication button on the Web screen, the client terminal 11 is in an authentication execution state. That is, the CPU 15 is in a state of controlling, for example, the operation software 23 to execute authentication. In this state, the CPU 15 notifies the living body information reading means 12 of a "living body information reading request". Then, the CPU 15 instructs the user to allow the living body information reading means 12 to read living body information through a displaying means and voice. An LED that displays the above instruction or a speaker emitting the voice may be provided separately. In addition, a similar instruction is issued to a high-order application through the interface 13. That is, the man-machine interface 13, such as a screen display of a personal computer and voice, is used to prompt the user to carry out reading operation of living body information.

[0100] Here, there are cases where a fingerprint information of quality of a certain standard cannot be obtained when dust and stain are attached on a surface of living body information such as a fingerprint, or on a surface of a scanner chip is stained in, for example, a fingerprint reading scanner. In such cases, reading of a fingerprint image is carried out until an image that satisfies quality of a certain standard is obtained.

[D]

Column 24, Line 17 to Column 25, Line 12

[0106] Here, when the pieces of living body information do not match with each other, the CPU 15 carries out display of "authentication is failed" and the like with respect to a high-order application through the interface 13 to notify the user. In contrast, when the pieces of living body information match with each other, the CPU 15 accesses the Internet passport area 21. Then, passport information can be obtained from the Internet passport area.

[0107] Details of the Internet passport area 21 will be described in a column of the Internet passport database 53 (of the second type) described later. Passport information is normally an ID or a passport for accessing the specific service site 40, or a card number of a settlement institution, such as a credit card company, a passport,

and the like. Hereinafter, description will be made by using the above information as the passport information.

[0108] In this case, the obtained passport information is transmitted from the client terminal 11 to the specific service site 40 in which the "authentication button" is clicked. The passport information of the specific service site 40 may be applied with encryption before being transmitted to the specific service site 40 as described later. Also, the system may be such that, in place of the passport information of the specific service site 40, other information (for example, authentication OK sign, or the like) may be applied with encryption and then transmitted. A case of applying encryption to the passport information of the specific service site 40 before transmission will be described in the description below.

[0109] When the client terminal 11 transmits the passport information of the specific service site 40 to the service site 40 site, an encryption processing function included in the operation software 23 applies encryption processing to the passport information. That is, an encrypting means is configured with the CPU 15, the operation software 23, the secret key PC-B, and the public key SS-A. In this encryption processing, the passport information (an ID and a passport, and the like) of the specific service site 40 is used as an original, and also one another copy of the same passport information is generated.

[0110] Then, the copy is compressed by using a hash function to create a digest version of the original. Then, a transmitter applies encryption to the digest version by using the own secret key PC-B. In this manner, the digest version becomes a digital signature. Further, the digital signature is attached to the original. When, both of the original and the attached digital signature are encrypted by using the public key SS-A on the service site 40 to conceal a transmission target. Then, after the above, the original and the digital signature are transmitted as encryption data to the service site 40 server side by SSL communication.

[E]

Column 27, Line 13 to Column 28, Line 41

[0123] Here, a configuration of data in the Web deposit 54 existing in the passport server 50 will be described based on FIG. 7 illustrated. Passport information shown in this figure is classified into levels described below based on access rights of the user. As shown in this figure, access rights of the user are classified into "Write permission right and deletion right", "Permission to know existence", "Permission to view content", "Permission to rewrite", "Permission to write once", and "Permission to use".

[0124] In addition, passport information of the user includes, for example, "Deposit ID", "Third-party institution description information", "Service site description information", "Public institution description information", "Private company description information", "User description information", "Living body information", and "Algorithm".

[0125] Access levels of the above passport information can be classified, for example, by setting flags. That is, a folder exclusively used, for example, for the deposit ID 30 is created, and a flag in property of the folder is set. For an access right to the deposit ID 30 being illustrated, the right of "Write permission right and deletion right" does not exist, and a flag corresponding to this right is set to "0". Also, since there is the right of "Permission to know existence", a flag corresponding to this right is set to "1".

[0126] In addition, in an another way of classifying access levels, a state capable of full access, in which all access rights are included, is shown by the number "0", and larger numbers are assigned as access rights are limited. In this case, numbers are

assigned for the number of combinations between columns from "Write permission right and deletion right" to "Permission to use" and rows from "Deposit ID" to "Algorithm", and access rights are corresponded to the numbers. In such a manner as well, control of access rights can be performed.

[0127] Since "Settlement institution information", "Service site information", and the like describe a plurality of pieces of settlement institution information and a plurality of pieces of service site information, folders for storing a plurality of pieces of information may be created and a flag is set for each of the folders.

[0128] As described above, as illustration of classifying access rights of the user, "o" shows permitted, "x" shows not permitted, and "Δ" shows permitted or not permitted depending on the principle of the service site 40. In this case, for "Deposit ID", "Write permission right and deletion right" is set to x, "Permitted to know existence" is set to o, "Permitted to view content" is set to o, "Permitted to rewrite" is set to x, "Permitted to write once" is set to x, and "Permitted to use" is set to o. In addition, for "Third-party institution description information", "Settlement institution information", "Service site description information", "Public institution description information", and "Private company description information", "Write permission right and deletion right" is set to o, "Permitted to know existence" is set to o, "Permitted to view content" is set to Δ, "Permitted to rewrite" is set to x, "Permitted to write once" is set to x, and "Permitted to use" is set to o.

[0129] Further, for "User description information", "Write permission right and deletion right" is set to o, "Permitted to know existence" is set to o, "Permitted to view content" is set to o, "Permitted to rewrite" is set to o, "Permitted to write once" is set to x, and "Permitted to use" is set to o. Also, for "Living body information", "Write permission right and deletion right" is set to x, "Permitted to know existence" is set to o, "Permitted to view content" is set to x, "Permitted to rewrite" is set to x, "Permitted to write once" is set to o, and "Permitted to use" is set to o. In addition, for "Algorithm", "Write permission right and deletion right" is set to x, "Permitted to know existence" is set to o, "Permitted to view content" is set to x, "Permitted to rewrite" is set to x, "Permitted to write once" is set to x, and "Permitted to use" is set to o.

[0130] However, setting of access rights is not limited to the ways in the above description, and an administrator of the Internet passport database 53 can set access rights in a variety of ways in consideration of importance of passport information.

[0131] When required passport information is pulled out to the passport server 50 from the deposit area configured as described above, the passport server 50 accesses a server of the specific service site 40 for which log-on is requested through the accessing means 51 based on the passport information. Log-on to the specific service site 40 is carried out based on URL transmitted together with the passport information.

対応なし、英抄

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-55959

(P2002-55959A)

(43)公開日 平成14年2月20日(2002.2.20)

(51) Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 4 9
17/60	2 2 2	17/60	2 2 2 5 B 0 5 5
	4 1 4		4 1 4 5 B 0 8 5
	5 0 4		5 0 4 5 J 1 0 4
	5 1 2		5 1 2

審査請求 未請求 請求項の数30 OL (全 23 頁) 最終頁に続く

(21)出願番号	特願2000-243787(P2000-243787)	(71)出願人	500239937 株式会社マックポート・バイオセキュリティ 東京都品川区西大井6丁目11番14号
(22)出願日	平成12年8月11日(2000.8.11)	(72)発明者	中野 裕二 東京都品川区西大井6丁目11番14号
		(74)代理人	100087859 弁理士 渡辺 秀治 (外1名)

最終頁に続く

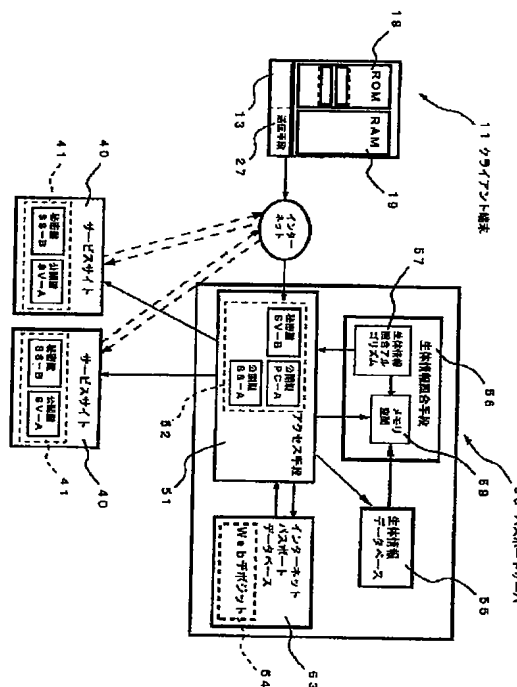
[最終頁に続く](#)

(54) 【発明の名称】 情報端末、認証システム及び認証方法

(57) 【要約】

【課題】 生体情報を用いたシングルサインのみで、容易にかつ絶対的な特定人の認証を可能とすると共に、他人が不正に生体情報を利用し得ない、セキュリティの極めて高い認証システム及び認証方法を提供すること。

【解決手段】 ネットワークを介して特定人に係る情報の管理を行い、その情報にアクセスする者が特定人か否かを認証する認証システム１０において、生体情報を読み取る生体情報読取手段１２と、特定人の生体情報を照合用として登録している生体情報登録手段５５と、生体情報登録手段５５と生体情報読取手段１２によって読み取られた生体情報との照合を行う生体情報照合手段５６と、生体情報登録手段に登録された生体情報と対応するように各サービスサイト４０のパスポート情報を記憶しているパスポート情報記憶手段５４と、生体情報が符合した場合にパスポート情報記憶手段５４から対応するパスポート情報を引き出して対応したサービスサイト４０にアクセスするアクセス手段５１と、を具備している。



【特許請求の範囲】

【請求項1】 ネットワークを介して特定人に係わる情報の管理を行い、その特定人に係わる情報にアクセスする者が特定人か否かを認証する認証システムにおいて、生体情報を読み取る生体情報読取手段と、特定人の生体情報を照合用として登録している生体情報登録手段と、

上記生体情報登録手段と上記生体情報読取手段によって読み取られた生体情報との照合を行う生体情報照合手段と、

上記生体情報登録手段に登録された生体情報と対応するように各サービスサイトの認証情報としてのパスポート情報を記憶しているパスポート情報記憶手段と、

上記生体情報照合手段によって登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、上記パスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、を具備することを特徴とする認証システム。

【請求項2】 前記生体情報読取手段によって読み取られ、前記生体情報照合手段との照合が為される生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、生体情報照合手段での生体情報の照合を行わないようにする照合回避手段が設けられていることを特徴とする請求項1記載の認証システム。

【請求項3】 前記読取生体情報記憶部、及び照合回避手段はパスポートサーバ内に設けられていることを特徴とする請求項2記載の認証システム。

【請求項4】 前記読取生体情報記憶部、及び照合回避手段は情報端末内に設けられていることを特徴とする請求項2記載の認証システム。

【請求項5】 前記生体情報登録手段、生体情報照合手段、パスポート情報記憶手段及びアクセス手段はパスポートサーバ内に設けられていることを特徴とする請求項1から4のいずれか1項に記載の認証システム。

【請求項6】 前記生体情報読取手段は情報端末内に設けられていると共に、この生体情報読取手段によって読み取られた生体情報は、情報端末内の送信手段によってパスポートサーバに伝送されることを特徴とする請求項5記載の認証システム。

【請求項7】 前記情報端末は、前記生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、

このデータ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、

前記パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、

上記特徴点抽出手段によって特徴点が抽出された生体情

報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開鍵で暗号化するための暗号化手段と、

を具備することを特徴とする請求項6記載の認証システム。

【請求項8】 前記生体情報が前記生体情報登録手段に登録されるに際して識別情報が割り当てられると共に、この識別情報は識別情報記憶部に記憶されており、前記生体情報照合手段での生体情報の照合を行うに先立って識別情報によって前記生体情報登録手段に登録されている生体情報を特定することを特徴とする請求項1から7のいずれか1項に記載の認証システム。

【請求項9】 前記識別情報記憶部は前記情報端末内部に設けられていることを特徴とする請求項8記載の認証システム。

【請求項10】 前記識別情報記憶部は前記情報端末内部に設けられていると共に、この識別情報記憶部に記憶されている識別情報は、前記生体情報と共に請求項4記載の暗号化手段によって暗号化されることを特徴とする請求項8記載の認証システム。

【請求項11】 前記パスポート情報記憶手段は、アクセスレベル別に分類されていることを特徴とする請求項1から10のいずれか1項に記載の認証システム。

【請求項12】 前記パスポート情報記憶手段のアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることを特徴とする請求項11記載の認証システム。

【請求項13】 前記アクセスレベルの設定は、フラグの設定によって行うことを特徴とする請求項11又は12記載の認証システム。

【請求項14】 前記アクセスレベルの設定は、アクセスレベル別に割り当てられた数字の設定によって行うことを特徴とする請求項11又は12記載の認証システム。

【請求項15】 前記パスポート情報記憶手段には、パスポート情報に対応したサービスサイトのURLも記憶されており、前記生体情報登録手段に登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、前記パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのURLも引き出し、このURLに基づいて前記アクセス手段で該サービスサイトにアクセスすることを特徴とする請求項1から14のいずれか1項に記載の認証システム。

【請求項16】 前記生体情報読取手段には、読み取ら

れた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることを特徴とする請求項 1 から 15 のいずれか 1 項に記載の認証システム。

【請求項 17】 ネットワークを介してパスポートサーバにアクセスすることが可能な情報端末において、生体情報を読み取る生体情報読取手段と、上記生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、上記データ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、上記特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開鍵で暗号化するための暗号化手段と、上記暗号化手段によって暗号化された生体情報をパスポートサーバ側に送信するための送信手段と、を具備することを特徴とする情報端末。

【請求項 18】 前記情報端末は、特定人の生体情報を照合用として登録している生体情報登録手段と、上記生体情報登録手段に登録された生体情報に対応するパスポート情報を記憶しているパスポート情報記憶手段と、前記生体情報読取手段によって読み取られ前記特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、上記生体情報照合手段での照合の結果、生体情報が符合した場合に上記パスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、を具備することを特徴とする請求項 17 記載の情報端末。

【請求項 19】 前記情報端末は、特定人の生体情報を照合用として登録している生体情報登録手段と、前記生体情報読取手段によって読み取られ前記特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、を具備して、上記生体情報照合手段での照合の結果、生体情報が符合した場合に符合情報を前記暗号化手段で前記生体情報に代えて暗号化し、この暗号化された生体情報を送信手段で送信することを特徴とする請求項 17 記載の情報端末。

【請求項 20】 前記情報端末には、この情報端末独自の識別情報が割り当てられていて、前記生体情報読取手

段で読み取られた生体情報を伝送手段で伝送するに際して識別情報も伝送することを特徴とする請求項 17 記載の情報端末。

【請求項 21】 前記生体情報読取手段によって読み取られた生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、前記送信手段から生体情報の送信を行わないようにする送信回避手段が設けられていることを特徴とする請求項 17 から 20 のいずれか 1 項に記載の情報端末。

【請求項 22】 前記生体情報読取手段には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることを特徴とする請求項 17 から 21 のいずれか 1 項に記載の情報端末。

【請求項 23】 ネットワークを介して特定人に係る情報の管理を行い、その特定人に係る情報にアクセスする者が特定人か否かを認証する認証方法において、生体情報を読み取る生体情報読取工程と、特定人の生体情報を照合用として登録している生体情報照合手段の生体情報と、上記生体情報読取工程によって読み取られた生体情報との照合を行う生体情報照合工程と、上記生体情報照合工程によって生体情報が符合した場合、この生体情報に対応するようにパスポート情報記憶手段に記憶されているパスポート情報を得るパスポート情報取得工程と、上記パスポート情報取得工程によって得られたパスポート情報に基づき、このパスポート情報に対応したサービスサイトにアクセスして該サービスサイトでのログオンを行うアクセス工程と、を具備することを特徴とする認証方法。

【請求項 24】 前記生体情報照合工程での生体情報の照合に先立って、照合用として登録している特定人の生体情報を識別情報に基づいて検索する識別手段検索工程を具備していることを特徴とする請求項 23 記載の認証方法。

【請求項 25】 前記生体情報登録工程、生体情報照合工程、パスポート情報記憶工程及びアクセス工程はパスポートサーバ内で行われることを特徴とする請求項 23 又は 24 記載の認証方法。

【請求項 26】 前記生体情報読取工程は情報端末内で行われると共に、この生体情報読取工程によって読み取られた生体情報は、情報端末内で行われる送信工程によってパスポートサーバ内に伝送されることを特徴とする請求項 25 記載の認証方法。

【請求項 27】 前記生体情報読取工程で読み取られた生体情報に対して、前記生体情報照合工程に先立って、前記生体情報読取手段によって読み取られた生体情報の

データ処理を行うデータ処理工程と、
上記データ処理工程によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出工程と、
上記特徴点抽出工程によって特徴点が抽出された生体情報を、前記パスポートサーバの鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの鍵情報記憶部に記憶されている公開鍵で暗号化する暗号化工程と、
を具備する請求項26記載の認証方法。

【請求項28】 前記パスポート情報取得工程により得られるパスポート情報は、前記パスポート情報記憶手段内部においてアクセスレベルに分類されて記憶されていることを特徴とする請求項23から27のいずれか1項に記載の認証方法。

【請求項29】 前記パスポート情報取得工程により得られるパスポート情報の前記パスポート情報記憶手段内部におけるアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができ
るレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワン
20 タイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることを特徴とする請求項28記載の認証方法。

【請求項30】 前記パスポート情報取得工程において、前記パスポート情報記憶手段にパスポート情報と共にこのパスポート情報に対応したURLも記憶されており、前記生体情報照合工程において生体情報が符合した場合に、前記パスポート情報記憶手段から対応するパス
30 ポート情報と共にサービスサイトのURLも引き出し、このURLに基づいて前記アクセス手段で該サービスサイトにアクセスすることを特徴とする請求項23から29のいずれか1項に記載の認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、生体情報を利用した認証システム及び認証方法に関する。

【0002】

【従来の技術】現在、個人の信用において商取引を行う場合には、その個人の認証を行うために種々の手段（トークン）を用いている。例えば、クレジットカードにおいては、暗証番号を用いたり、或いはサイン等を用いてカード使用者が本人であるか否かの確認を行っている。

【0003】現在、個人の身分を証明する場合、身分証明を提示する場によって、リアル世界の身分証明手段、準バーチャル世界の身分証明手段、及びバーチャル世界の身分証明手段の三段階に分けられる。このうち、リアル世界における身分証明手段とは、従前から存在する身分証明手段であり、基本的には身分証明手段を有する個
50

人を対面にて身分照合するものである。

【0004】このリアル世界の身分証明手段としては、例えば学生であれば学生証、会社員であれば社員証、車の運転を行う人の場合には運転免許証、海外旅行を行う人の場合にはパスポート等がある。さらに、他にはクレジット決済を行う人の場合にはクレジットカードとサイン、或いは病院に通院する場合に必要な健康保険証、さらには各種会員証、ポイントカード等がある。

【0005】また、準バーチャル世界の身分証明手段とは、所定の箇所に存する端末からオンラインを介して身分照合を行うものである。この準バーチャル世界の身分証明手段としては、銀行のATMにおいて銀行のキャッシュカードとパスワードによるものがある。さらに、バーチャル世界の身分証明手段とは、近年急速に普及したインターネット等のネットワークを介しての身分照合を行うものである。バーチャル世界の身分証明手段としては、インターネット接続のプロバイダーにおける会員IDとパスワード、会社のパソコンにおけるIDとパスワード、ショッピングモールにおける会員IDとパスワードがある。また、他には、PKI（Public Key Infrastructure）技術を適用した身分証明手段もある。

【0006】

【発明が解決しようとする課題】ところで、リアル世界の身分証明手段では、持ち物による所有者認証、顔写真による目視認証を行い、またクレジットカードにおいてはサイン癖による目視認証を行っている。すなわち、個人と個人とが対面するため、かかる身分証明手段で混乱のない商取引が実現されている。かかるリアル世界で身分を偽装するためには、（1）偽造組織（人）、（2）偽造技術、（3）資本、（4）費用対効果、（5）他人の身分証明手段を複製し、それを短時間で利用する高度なビジネスモデル、の夫々が必要とされる。また、身分証明手段を偽造できたとしても、身分証明手段の利用箇所に監視カメラが設置されている場合が多く、かかる監視カメラでの録画により、例え不正を行ったとしても後日録画内容を検索することができる。それ故、リアル世界では、偽装が困難であり、よって現状の身分証明手段で混乱のない商取引が実現されている。

【0007】また、準バーチャル世界の身分証明手段では、例えばキャッシュカードとパスワードにより認証を行っている。この場合、キャッシュカードという持ち物、及びパスワードの記憶の二つの手段により、本人か否かの認証を行っている。それ故、パスワードを忘れてしまうと該キャッシュカードが利用できなくなる、といった問題を有している。

【0008】また、パスワードを盗まれた場合には、キャッシュカードを盗むだけで簡単に特定人に成りすますことが可能となる。さらに、特に複数のキャッシュカードを持った場合に顕著であるが、パスワードは忘れやすいものである故、パスワードを特定人の個人属性（例え

ば誕生日等)にして記憶している場合が多い。それ故、他人は特定人のパスワードを容易に推測できる場合が多い。しかしながら、準バーチャル世界においても、例えばATMの設置箇所には監視カメラが設置されている場合がほとんどであり、偽装しても後日録画内容を検索することが可能である。

【0009】また、バーチャル世界の身分証明手段では、インターネット等のネットワークを介して特定人か否かの認証を行うことが必要とされる。かかるインターネットにおいては、対面でないため顔を確認することができない。また、監視カメラで撮影することもできない。さらには、インターネットにおいては匿名で活動することが許されている。それ故、相手方がどこに住んでいるかさえも分からない、といった問題を有している。

【0010】このようなバーチャル世界の身分証明手段では、例えばIDとパスワードにより認証する場合、或いはPKIの秘密鍵を保持しこれを用いて認証する場合がある。しかしながら、IDとパスワードにより認証する場合、IDやパスワードを忘れてしまうと利用できない、といった問題を有している。それ故、パスワードを個人属性にすることが多く、他人が容易にパスワードを推測することができる、といった準バーチャル世界と同様の問題を有している。また、IDやパスワードが盗まれると、簡単に他人が特定人に成りすますことができる。

【0011】さらに、PKIの秘密鍵を用いて認証する場合、この秘密鍵が他人に盗まれると成りすましが防止できない、といった問題を有している。すなわち、PKIを特定の記憶メディアや情報端末に保存した場合、この秘密鍵が盗まれると、公開鍵により暗号化されたデータが容易に復号化されてしまう。また、秘密鍵により暗号化してデータを送信し、受信した相手の公開鍵で復号化すると、データが誰から送られてきたのかを認証することができるが、厳密に言えば、秘密鍵を保存している記憶メディアや情報端末を認証するのみである。それ故、他人が秘密鍵を不正に入手した場合には、特定人に成りすますことが可能となってしまう。すなわち、特定人であることの絶対的な認証は、PKI方式では行えない。

【0012】さらに、バーチャル世界では、リアル世界及び準バーチャル世界のように監視カメラで録画することがないため、他人が特定人に成りすます場合のリスクが、リアル世界及び準バーチャル世界と比較して非常に高いものとなっている。

【0013】特に近年は、インターネットの急速な発展・普及により、インターネットを介したオンラインショッピング等の電子商取引が徐々に活発化するようになってきている。かかる電子商取引においては、本人であるか否かを確実に認証する必要がある。しかしながら、電子商取引の現状においては、例えばクレジットカードの

カード番号と暗証番号を確認することにより、本人であるか否かの認証を行っている。このため、かかるカード番号や暗証番号が他人に知られた場合、成りすましを防ぐことができず、リスクの高い商取引手段とならざるを得ないのが現状である。また、このような認証事故によるリスクを回避するために、クレジットカード会社等の債権回収業者は、保険会社との契約を行うのが通常である。かかる保険契約では、認証事故の頻度がリアル世界と比較して大きいため、保険料が高額となり、これが価格低下の妨げとなっている。

【0014】また、電子商取引以外にも、例えば行政庁・各役所に対する手続をインターネットを介して行えるようにする、いわゆる電子政府の構想があり、例えばシンガポールのように、既に実用段階に踏み切っている国も存在する。また、我が国も、2003年度に電子政府の実現へ向けて準備を進めている。このような電子政府構想においても、特定人であるか否かを確実に認証する必要がある、かかる特定人であることの認証が確実に為されないと、他人がプライバシーを侵害してしまったり、個人の財産・権利等に係わる問題を生じてしまう場合がある。このため、日本においては、現状ではまだ実用化がなされていなく、一部で実験的に導入されているのみである。

【0015】以上のことをまとめると、図8のようになる。この図に示すように、バーチャル世界においての特定人か否かの認証は、記憶手段に記憶された情報に基づく認証である。ここで、例えばICカードのようなハードウェア手段を所持している所持者が真の所有者であるか否かの確認は行えず、またハードウェア手段が偽造されたものであるか否かの真偽を確認することができない。よって、最終的にはソフトウェアのみで行う必要がある。さらに、かかるソフトウェアによる認証において、認証事故がなく精度良く行えるようにする必要がある。

【0016】上述のような特定人であるか否かの認証が確実に行われるようになれば、インターネットを介しての電子商取引、或いは電子政府構想が一般化・現実化するものとなり、かかる認証を行える認証システム、認証方法が待望されている。また、その認証が複雑でなく、誰でも行えるように簡便化されるものが待望されている。

【0017】本発明は、上記の事情に基づきなされたもので、その目的とするところは、生体情報を用いたシングルサインのみで、容易にかつ絶対的な特定人の認証を可能とすると共に、他人が不正に生体情報を利用し得ない、セキュリティの極めて高い認証システム及び認証方法を提供しよう、とするものである。

【0018】

【課題を解決するための手段】 上述の目的を達成するため、本発明は、ネットワークを介して特定人に係わる情

報の管理を行い、その特定人に係る情報にアクセスする者が特定人か否かを認証する認証システムにおいて、生体情報を読み取る生体情報読取手段と、特定人の生体情報を照合用として登録している生体情報登録手段と、生体情報登録手段と生体情報読取手段によって読み取られた生体情報との照合を行う生体情報照合手段と、生体情報登録手段に登録された生体情報と対応するように各サービスサイトの認証情報としてのパスポート情報を記憶しているパスポート情報記憶手段と、生体情報照合手段によって登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、パスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、を具備することとしたものである。

【0019】このため、生体情報を生体情報読取手段で読み取り、特定人の生体情報と符合すれば、パスポート情報記憶手段に記憶されているパスポート情報を引き出して、アクセス手段によってこのパスポート情報に対応したサービスサイトにアクセスすることが可能となる。すなわち、生体情報の読み取りのみによって所定のサービスサイトにアクセス可能となり、複数のサービスサイトのIDやパスワードに対応させることができる。このため、一々複数のIDやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイトの認証を行うことが可能となる。すなわち、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイトでの認証を行うことが可能となる。

【0020】また、他の発明は、上述の発明に加えて更に、生体情報読取手段によって読み取られ、生体情報照合手段との照合が為される生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、生体情報照合手段での生体情報の照合を行わないようにする照合回避手段が設けられていることとしたものである。

【0021】このため、一度読み取られた生体情報を読取生体情報記憶部に記憶させておき、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報に基づく照合を、照合回避手段で拒否することができる。すなわち、他人が不正に特定人の生体情報を入手した場合、その生体情報を用いて生体情報の照合を行おうとしても、読取生体情報記憶部に記憶されている生体情報を用いることはできない。これは、例えば指紋のような生体情報では、押圧角度や押圧面積、或いは押圧力が同じである全く同一の生体情報が得られることはほとんどないことに基づくものである。

【0022】さらに、他の発明は、上述の発明に加えて

更に、読取生体情報記憶部、及び照合回避手段はパスポートサーバ内に設けられていることとしたものである。このため、パスポートサーバにおいて一度照合した生体情報を蓄えておくことができ、この蓄えられた生体情報と同一の生体情報がパスポートサーバに送信されてきた場合には、照合回避手段で生体情報の照合を回避することが可能となる。

【0023】また、他の発明は、上述の発明に加えて更に、読取生体情報記憶部、及び照合回避手段は情報端末内に設けられることとしたものである。このため、情報端末内部に一度照合した生体情報を蓄えておくことができ、この蓄えられた生体情報と同一の生体情報が生体情報読取手段で読み取られた場合には、照合回避手段で生体情報の照合を回避することが可能となる。すなわち、クライアント端末側で、照合回避手段を働かせることが可能となる。

【0024】さらに、他の発明は、生体情報登録手段、生体情報照合手段、パスポート情報記憶手段及びアクセス手段はパスポートサーバ内に設けられていることとしたものである。

【0025】このため、同一のパスポートサーバ内で、生体情報の照合や、それに対応したパスポート情報を引き出してアクセス手段でサービスサイトにアクセスする。それにより、アクセス速度を速くすることが可能となる。

【0026】また、他の発明は、生体情報読取手段は情報端末内に設けられていると共に、この生体情報読取手段によって読み取られた生体情報は、情報端末内の送信手段によってパスポートサーバに伝送されることとしたものである。

【0027】このため、情報端末単独で生体情報の読み取りを行い、この情報端末によって読み取られた生体情報を情報端末内の送信手段によって伝送する。それにより、ユーザが所持可能な情報端末を用いてネットワークを介して簡易に生体情報による認証を行い、この生体情報とパスポート情報を対応させることで、生体情報をシングルサイン感覚で簡易に身分証明手段として用いることが可能となる。

【0028】さらに、他の発明は、情報端末は、生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理手段と、このデータ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開鍵で暗号化するための暗号化手段と、を具備することとしたものである。

【0029】このため、生体情報読取手段によって読み取られた生体情報を、まずデータ処理手段によるデータ

処理を行う。続いて、データ処理手段でデータ処理が為された生体情報に対して、特徴点抽出手段で特徴点の抽出を行う。そして、特徴点抽出された生体情報に対して、暗号化手段を用いて鍵情報記憶部に記憶されている独自の秘密鍵で暗号化した後に、パスポートサーバの公開鍵で暗号化を行う。このような状態でパスポートサーバ側に伝送すれば、例えば伝送経路の途中で他人が不正に生体情報を入手しても、秘密鍵及び公開鍵で暗号化が為されているので、解読が極めて困難なものとなり、生体情報の伝送に際しての安全性を確保することが可能となる。また、情報端末独自の秘密鍵で暗号化した後に、パスポートサーバ側の公開鍵で暗号化するので、伝送経路の途中で他人が不正に生体情報を入手し、入手した生体情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますることが不可能となる。

【0030】また、他の発明は、上述の各発明に加えて更に、生体情報が生体情報登録手段に登録されるに際して識別情報が割り当てられると共に、この識別情報は識別情報記憶部に記憶されており、生体情報照合手段での生体情報の照合を行うに先立って識別情報によって生体情報登録手段に登録されている生体情報を特定することとしたものである。

【0031】このため、生体情報照合手段での照合を行うに先立って、識別情報に基づいて生体情報登録手段に登録されている生体情報を引き出すことが可能となる。すなわち、かかる識別情報での生体情報の検索を行うことによって、生体情報の照合を行う際の時間の短縮を図ることが可能となる。

【0032】さらに、他の発明は、上述の発明に加えて更に、識別情報記憶部は前記情報端末内部に設けられていることとしたものである。このため、情報端末で生体情報の読み取りを行い、この生体情報を情報端末から伝送するに際して、識別情報を識別情報記憶部から呼び出して一緒に伝送することとなる。このように、識別情報記憶部を情報端末に設けることで、一々特定人が識別情報を入力しなくても、生体情報の読取を行えば、この生体情報の読み取りと共に生体情報の伝送を行うことが可能となる。

【0033】また、他の発明は、上述の発明に加えて更に、識別情報記憶部は情報端末内部に設けられていると共に、この識別情報記憶部に記憶されている識別情報は、生体情報と共に暗号化手段によって暗号化されることとしたものである。

【0034】このため、生体情報のみならず、識別情報を他人が不正に伝送経路途中で入手しても、その内容を秘匿化することが可能となり、識別情報の解読が極めて困難となって安全性を確保することが可能となる。ま

た、識別情報に対しても情報端末独自の秘密鍵で暗号化した後に、パスポートサーバ側の公開鍵で暗号化するので、伝送経路の途中で他人が不正に識別情報を入手し、入手した識別情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますることが不可能となる。

【0035】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報記憶手段は、アクセスレベル別に分類されていることとしたものである。この場合、パスポート情報は、生体情報と対応するように設けられているので、生体情報読取手段によって生体情報を読み取らせると、この生体情報に対応したパスポート情報を引き出すことができる。この場合、IDやパスワードの如き単なる情報ではなく、生体情報を自己の身分証明手段として用いて認証を行うため、他人が特定人に成りすますのを防止することができる。

【0036】さらにユーザのアクセスレベルの設定により、ネットを介しての会員制サービスサイト、或いは決済機関、公的機関、民間企業等が運営する、種々のサービスサイトにメリットが生ずることとなる。例えば、決済機関の情報を記載している場合、ユーザのアクセスレベルを「存在を知ることができる」を○として、「書換えできる」を×とした場合、ユーザは勝手にパスポート情報であるIDやパスワードを書き換えることができない。このようなアクセスレベルの設定により、各サイト側において生体情報を活用した本人の絶対認証を現実的に利用可能となる。

【0037】また、例えばデータを保存する領域をパスポート情報記憶手段内に設けた場合、アクセスレベルの設定の仕方によってはデータの保存はできるがコピーはできないようにすることもできる。この場合には、特定人は生体情報を用いてアクセス可能となり、パスポート情報記憶手段内でそのデータをアクセスレベルに設定されたレベル内で利用可能となるが、違法なコピー等は行えないものとなる。それによって、種々のコンテンツからデータを該パスポート情報記憶手段内にダウンロードした場合、他の領域にはコピーできないため、該データの著作権を守ることが可能となる。

【0038】また、他の発明は、上述の発明に加えて更に、パスポート情報記憶手段のアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることとしたものである。

【0039】このように各レベルに分けて分類したことにより、夫々のサービスサイトが要求する状態に、ユーザのアクセス権利を制限することが可能となる。これによって、生体情報の読み取りで該パスポート情報記憶手段にアクセスした場合、ユーザに対してもIDやパスワードの秘匿性を確保することも可能となる。

【0040】さらに、他の発明は、上述の各発明に加えて更に、アクセスレベルの設定は、フラグの設定によって行うこととしたものである。このようにフラグの設定によりアクセスレベルを種々設定するので、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにパスポート情報記憶手段を設定できる。

【0041】また、他の発明は、上述の各発明に加えて更に、アクセスレベルの設定は、アクセスレベル別に割り当てられた数字の設定によって行うこととしたものである。このようにアクセスレベル別に割り当てられた数字の設定によってアクセスレベルを種々設定するので、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにパスポート情報記憶手段を設定することができる。

【0042】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報記憶手段には、パスポート情報に対応したサービスサイトのURLも記憶されており、生体情報登録手段に登録された生体情報と、生体情報読取手段によって読み取られた生体情報とが符合した場合に、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのURLも引き出し、このURLに基づいてアクセス手段で該サービスサイトにアクセスすることとしたものである。

【0043】このため、生体情報照合手段での照合で生体情報が符合した場合、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのURLを引き出して、このURLに基づいてアクセス手段で特定のサービスサイトにアクセスすることが可能となる。すなわち、一々URLを検索したり入力せずに、特定のサービスサイトにアクセス可能となる。

【0044】また、他の発明は、上述の発明に加えて更に、生体情報読取手段には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段が設けられていることとしたものである。このため、生体情報により特定人か否かの照合を行う場合、基準の品質以上の生体情報にて特定人か否かの認証を行える。それによって、例えば生体情報読取手段の汚れによって一定基準以下の生体情報に基づく認証を行うのを防止することができ、認証精度の向上を図ることができる。

【0045】また、他の発明は、ネットワークを介してパスポートサーバにアクセスすることが可能な情報端末において、生体情報を読み取る生体情報読取手段と、生体情報読取手段によって読み取られた生体情報のデータ

処理を行うデータ処理手段と、データ処理手段によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出手段と、パスポートサーバの公開鍵、及び独自の秘密鍵を記憶している鍵情報記憶部と、特徴点抽出手段によって特徴点が抽出された生体情報を、鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの公開で暗号化するための暗号化手段と、暗号化手段によって暗号化された生体情報をパスポートサーバ側に送信するための送信手段と、を具備することとしたものである。

【0046】このように、生体情報読取手段によって読み取られた生体情報をデータ処理手段及び特徴点抽出手段を介して特徴点の抽出を行う。さらに、特徴点の抽出が為された生体情報に対して暗号化手段により独自の秘密鍵、及びパスポートサーバの公開鍵で暗号化する。すなわち、本人であるか否かの絶対的な認証を行える生体情報を用い、さらにこの生体情報に対して、どの情報端末から送信されたかを特定するための秘密鍵で暗号化する。そのため、特定人を生体情報で特定可能であると共に、秘密鍵によって端末認証も行える。さらに、生体情報を秘密鍵で暗号化した後に、パスポートサーバの公開鍵で暗号化を行うので、秘密鍵を有しているパスポートサーバのみしか復号化を行えない。それによって、生体情報の秘匿性を保つことが可能となる。

【0047】さらに、他の発明は、上述の発明に加えて更に、情報端末は、特定人の生体情報を照合用として登録している生体情報登録手段と、生体情報登録手段に登録された生体情報に対応するパスポート情報を記憶しているパスポート情報記憶手段と、生体情報読取手段によって読み取られ特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、生体情報照合手段での照合の結果、生体情報が符合した場合にパスポート情報記憶手段から対応するパスポート情報を引き出し、このパスポート情報に対応したサービスサイトにアクセスするアクセス手段と、を具備することとしたものである。

【0048】このため、生体情報読取手段によって読み取らせた生体情報を、生体情報照合手段によって照合することが可能となる。すなわち、情報端末側で特定人か否かの認証が行える、クライアント端末認証型の情報端末にすることができる。さらに、生体情報が照合した場合に、パスポート情報記憶手段から対応するパスポート情報を引き出して、このパスポート情報に対応したサービスサイトにアクセス手段でアクセスすることができる。このようにすることで、情報端末側において各サービスサイトでの認証を行って、該サービスサイトにログオンすることが可能となる。

【0049】また、他の発明は、上述の発明に加えて更に、情報端末は、特定人の生体情報を照合用として登録

している生体情報登録手段と、生体情報読取手段によって読み取られ特徴点抽出手段によって特徴点が抽出された生体情報と生体情報登録手段に照合用として登録されている生体情報との照合を行うための生体情報照合手段と、を具備して、生体情報照合手段での照合の結果、生体情報が符合した場合に符合情報を暗号化手段で生体情報に代えて暗号化し、この暗号化された生体情報を送信手段で送信することとしたものである。

【0050】このため、生体情報読取手段で読み取られた生体情報に基づいて、特定人であるか否かの認証を生体情報照合手段で情報端末側で行うことが可能となる。また、特定人であるとの認証が為された場合、符合情報を暗号化手段で暗号化した後に送信手段で送信するので、符合情報の安全性、秘匿性を確保することが可能となる。

【0051】さらに、他の発明は、上述の発明に加えて更に、情報端末には、この情報端末独自の識別情報が割り当てられていて、生体情報読取手段で読み取られた生体情報を伝送手段で伝送するに際して識別情報も伝送することとしたものである。

【0052】このため、パスポートサーバ側において生体情報照合手段での照合を行うに先立って、識別情報に基づいて生体情報登録手段に登録されている生体情報を引き出すことが可能となる。すなわち、かかる識別情報での生体情報の検索を行うことによって、生体情報の照合を行う際の時間の短縮を図ることが可能となる。

【0053】また、他の発明は、上述の各発明に加えて更に、生体情報読取手段によって読み取られた生体情報を記憶するための読取生体情報記憶部が設けられると共に、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、前記送信手段から生体情報の送信を行わないようにする送信回避手段が設けられていることとしたものである。

【0054】このため、一度読み取られた生体情報を読取生体情報記憶部に記憶させておき、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報が読み取られた場合、送信回避手段によって生体情報の送信を拒否することができる。すなわち、他人が不正に特定人の生体情報を入手した場合、その生体情報を用いて生体情報の照合を行おうとしても、読取生体情報記憶部に記憶されている生体情報は用いることはできない。これは、例えば指紋のような生体情報では、押圧角度や押圧面積、或いは押圧力が同じである全く同一の生体情報が得られることはほとんどないことに基づくものである。このため、一度用いられた生体情報と全く同一の生体情報を再度用いることを防止することができる。

【0055】さらに、他の発明は、上述の各発明に加えて更に、生体情報読取手段には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行

うようにする生体情報判別手段が設けられていることとしたものである。

【0056】このため、生体情報により特定人か否かの照合を行う場合、基準の品質以上の生体情報にて特定人か否かの認証を行える。それによって、例えば生体情報読取手段の汚れによって一定基準以下の生体情報に基づく認証を行うのを防止することができ、認証精度の向上を図ることができる。

【0057】また、他の発明は、ネットワークを介して特定人に係る情報の管理を行い、その特定人に係る情報にアクセスする者が特定人か否かを認証する認証方法において、生体情報を読み取る生体情報読取工程と、特定人の生体情報を照合用として登録している生体情報照合手段の生体情報と、生体情報読取工程によって読み取られた生体情報との照合を行う生体情報照合工程と、生体情報照合工程によって生体情報が符合した場合、この生体情報に対応するようにパスポート情報記憶手段に記憶されているパスポート情報を得るパスポート情報取得工程と、パスポート情報取得工程によって得られたパスポート情報に基づき、このパスポート情報に対応したサービスサイトにアクセスして該サービスサイトでのログオンを行うアクセス工程と、を具備することとしたものである。

【0058】このため、生体情報を生体情報読取工程で読み取らせ、特定人の生体情報と符合すれば、パスポート情報記憶手段に記憶されているパスポート情報をパスポート情報取得工程で引き出して、アクセス工程によってこのパスポート情報に対応したサービスサイトにアクセスすることが可能となる。すなわち、生体情報の読み取りのみによって所定のサービスサイトにアクセス可能となり、複数のサービスサイトのIDやパスワードに対応させることができる。このため、一々複数のIDやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイトの認証を行うことが可能となる。すなわち、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイトでの認証を行うことが可能となる。

【0059】さらに、他の発明は、上述の発明に加えて更に、生体情報照合工程での生体情報の照合に先立って、照合用として登録している特定人の生体情報を識別情報に基づいて検索する識別手段検索工程を具備していることとしたものである。

【0060】このため、生体情報照合工程での照合に先立って、識別情報に基づいて登録されている生体情報を引き出すことが可能となる。すなわち、かかる識別情報に基づいて生体情報の検索を行うことによって、生体情報の照合を行う際の時間の短縮を図ることが可能となる。

【0061】また、他の発明は、上述の各発明に加えて

10

20

30

40

50

更に、生体情報登録工程、生体情報照合工程、パスポート情報記憶工程及びアクセス工程はパスポートサーバ内で行われることとしたものである。

【0062】このため、同一のパスポートサーバ内で、生体情報の照合や、それに対応したパスポート情報を引き出してアクセス工程によってサービスサイトにアクセスする。それによって、アクセス速度を速くすることが可能となる。

【００６３】さらに、他の発明は、上述の発明に加えて更に、生体情報読取工程は情報端末内で行われると共に、この生体情報読取工程によって読み取られた生体情報は、情報端末内で行われる送信工程によってパスポートサーバ内に伝送されることとしたものである。

【0064】このため、情報端末単独で生体情報の読み取りを行い、この情報端末によって読み取られた生体情報を情報端末内の送信手段によって送信する。それにより、ユーザが所持可能な情報端末を用いて簡易に生体情報による認証を行い、この生体情報とパスポート情報との対応により、ユーザは生体情報をシングルサイン感覚で簡易に用いることが可能となる。

【0065】また、他の発明は、上述の発明に加えて更に、生体情報読取工程で読み取られた生体情報に対して、生体情報照合工程に先立って、生体情報読取手段によって読み取られた生体情報のデータ処理を行うデータ処理工程と、データ処理工程によってデータ処理が為された生体情報から特徴点を抽出する特徴点抽出工程と、特徴点抽出工程によって特徴点が抽出された生体情報を、パスポートサーバの鍵情報記憶部に記憶されている独自の秘密鍵で暗号化するとともに、その後にパスポートサーバの鍵情報記憶部に記憶されている公開鍵で暗号化する暗号化工程と、を具備することとしたものである。

【0066】このため、生体情報読取工程によって読み取られた生体情報に対して、まずデータ処理工程によってデータ処理を行う。続いて、データ処理工程でデータ処理が為された生体情報に対して、特徴点抽出工程で特徴点の抽出を行う。そして、特徴点が抽出された生体情報に対して、暗号化工程によって鍵情報記憶部に記憶されている独自の秘密鍵で暗号化した後に、パスポートサーバの公開鍵で暗号化を行う。このようにしてパスポートサーバに伝送すれば、例えば伝送経路の途中で他人が不正に生体情報を入手しても、秘密鍵及び公開鍵で暗号化が為されているので、解読が極めて困難なものとなり、生体情報の伝送に際しての安全性を確保することができる。また、情報端末独自の秘密鍵で暗号化した後に、パスポートサーバ側の公開鍵で暗号化するので、伝送経路の途中で他人が不正に生体情報を入手し、入手した生体情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。

すなわち、事実上、特定人に成りすますることが不可能となる。

【0067】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報取得工程により得られるパスポート情報は、パスポート情報記憶手段内部においてアクセスレベルに分類されて記憶されていることとしたものである。

【0068】このため、パスポート情報は、生体情報と対応するように設けられているので、生体情報読取工程において読み取られた生体情報に基づいて、この生体情報に対応したパスポート情報を引き出すことが可能となる。この場合、IDやパスワードの如き単なる情報ではなく、生体情報を自己の身分証明手段として用いて認証を行うため、他人が特定人に成りすますのを防止することが可能となる。

【0069】また、他の発明は、上述の発明に加えて更に、パスポート情報取得工程により得られるパスポート情報の前記パスポート情報記憶手段内部におけるアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワнтаイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されていることとしたものである。

【0070】このように各レベルに分けて分類したことにより、夫々のサービスサイトが要求する状態に、ユーザのアクセス権利を制限することが可能となる。これによって、生体情報の読み取りで該パスポート情報記憶手段にアクセスした場合、ユーザに対してもIDやパスワードの秘匿性を確保することも可能となる。

【0071】さらに、他の発明は、上述の各発明に加えて更に、パスポート情報取得工程において、パスポート情報記憶手段にパスポート情報と共にこのパスポート情報に対応したURLも記憶されており、生体情報照合工程において生体情報が符合した場合に、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのURLも引き出し、このURLに基づいてアクセス手段で該サービスサイトにアクセスすることとしたものである。

【0072】このため、生体情報照合工程での照合で生体情報が符合した場合、パスポート情報記憶手段から対応するパスポート情報と共にサービスサイトのURLを引き出して、このURLに基づいてアクセス工程で特定のサービスサイトにアクセスすることが可能となる。すなわち、一々URLを検索したり入力するせずに、特定のサービスサイトにアクセス可能となる。

【0073】

【発明の実施の形態】以下、本発明の一実施の形態について、図1から図7に基づいて説明する。

【0074】図6は、本発明の認証システム10の概略を示すシステム図である。この図において、個人Aは情報端末としてのクライアント端末11を有している。クライアント端末11には、例えばパーソナルコンピュータや、WEB対応の携帯電話端末、或いは携帯情報端末(PDF)がある。

【0075】クライアント端末11は、内部に生体情報読取手段12を具備しており、この生体情報読取手段12にて指紋等の生体情報の読み取りを行う構成である。ここで、生体情報読取手段12により読み取られる生体情報には、指紋、虹彩、人のサイン、掌形、顔形、耳形、体臭、指の長さ、静脈の血管パターン、DNA、声紋等がある。このうち、生体情報読取手段12は、いずれかの生体情報を読み取れるように構成されている。代表的な生体情報読取手段12としては、指紋認証スキャナや掌形認証スキャナ等がある。そして、クライアント端末11には、かかる指紋認証スキャナ等の生体情報読取手段12が内蔵されたり、或いはインターフェース13を介して外部から取り付けられる。

【0076】生体情報読取手段12は、データ処理手段としてのDSP14(Digital Signal Processor)やCPU15(中央演算処理装置)等と接続されている。そして、生体情報読取手段12の全ての行動は、CPU15によって監視される状態となる。

【0077】指紋スキャナチップ等の生体情報読取手段12は、DSP14に接続されている。DSP14は、生体情報読取手段12によって読み取られたデジタルデータである生体情報の画像データ処理の演算を、高速で行うための回路である。この画像データ処理は、画像の細線化と2値化を行うものであり、例えば所定の太さを有する指紋を細くしたり、白黒のコントラスト8階調からなる画像データを、いずれかのしきい値で白と黒の2階調に分けるためのものである。

【0078】そして、DSP14はCPU15に接続されている。このCPU15は、さらにメモリ領域16とインターフェース13を介して接続されている。メモリ領域16は、RAM17とROM18を有している。このうち、RAM17は不揮発性メモリであり、データの読み込みや書き込み、及びデータの書き換えを自由に行える、といった通常のRAMが具備している性質を備えていると共に、電源を切っても記憶されているデータが消滅しない、といった性質を有しているメモリである。

【0079】ここで、メモリ領域16のRAM17とROM18の内部構成として、以下の3パターンの構成が存在する。

【0080】その1つ目は、図1に示すようなクライアント端末認証型の構成であり、クライアント端末11内部で認証を行って、インターネットパスポートを取得す

るものである。このクライアント端末認証型のメモリ領域16の構成は、RAM17に指紋特徴点データ等の生体情報特徴点データ20が存在し、またこれと共にインターネットパスポート領域21、及びワーク領域22が存在する構成である。このうち、インターネットパスポート領域21は、パスポート情報記憶手段としての役割を果たすものであり、電源を切っても消滅しないようになっている。

【0081】また、ROM18には、オペレーションソフトウェア23、特徴点抽出アルゴリズム24、生体情報照合アルゴリズム25、及び秘密鍵PC-B、公開鍵SS-Aを記憶している鍵情報記憶部26が格納されている。さらに、生体情報特徴点データ20は、特定人の生体情報を照合用として登録しているものであり、生体情報登録手段としての機能を果たすものである。

【0082】このうち、オペレーションソフトウェア23は、情報端末が電源ONとなったときに、最初にCPU15に読み込まれるものである。このオペレーションソフトウェア23には、上位アプリケーション、及び下位アプリケーションが存している。

【0083】また、同じくROM18には、特徴点抽出手段としての特徴点抽出アルゴリズム24が記憶されている。特徴点抽出アルゴリズム24は、生体情報読取手段12によって読み取られた生体情報から、特徴点の抽出を行うものである。そして、抽出された生体情報の特徴点は、照合用として予めRAM17内に記憶されている。

【0084】また、ROM18には、生体情報照合アルゴリズム25が記憶されている。生体情報照合アルゴリズム25は、生体情報読取手段12によって読み取られ特徴点抽出アルゴリズム24によって抽出された特徴点と、照合用の生体情報特徴点データ20との照合を行う、生体情報照合手段としての機能を果たすものである。この生体情報照合アルゴリズム25によって、生体情報読取手段12で読み取られた生体情報が、特定人のものであるか否かの確認が行える構成である。

【0085】なお、生体情報読取手段12で読み取られ生体情報照合アルゴリズム25で照合がなされた生体情報を記憶する読取生体情報記憶部を別途設け、さらにこの読取生体情報記憶部に記憶されている生体情報と同一の生体情報が生体情報読取手段から読み取られた場合に、生体情報照合アルゴリズム25での照合を行わないようにする照合回避手段を設ける構成にしても構わない。

【0086】また、ROM18には、鍵情報記憶部26が設けられている。この鍵情報記憶部26には、暗号化手段としての秘密鍵PC-B及び公開鍵SS-Aが記憶されている。秘密鍵PC-Bは、クライアント端末11が特有に有しているものであり、他には同一のものは存在しない。また、秘密鍵PC-Bは、サービスサイト4

0側に存する公開鍵PC-Aと対を成す構成である。すなわち、秘密鍵PC-Bにより暗号化・復号化したデータは、サービスサイト40側の公開鍵PC-Aによって復号化・暗号化されるようになっている。さらに、公開鍵SS-Aは、サービスサイト40側の秘密鍵SS-Bと対を成す構成であり、サービスサイト40側の秘密鍵SV-Bに対応した複数のものが存在する。公開鍵SV-Aによって暗号化・復号化したデータは、サービスサイト40側の秘密鍵SV-Bによってのみ復号化・暗号化されるようになっている。

【0087】これら秘密鍵PC-B26及び公開鍵SS-Aは、ROM18内部に耐タンパー性を持たせて記憶されている。すなわち、ROM18は例えばワンチップのLSI内部に存するものであり、このワンチップ化されたLSI内部に秘密鍵PC-B26と公開鍵SS-Aが記憶され、それによって十分な耐タンパー性を持たせて構成されているものである。それ故、このROM18から秘密鍵PC-B及び公開鍵SS-Aを読み取ることは、ほぼ不可能となっている。

【0088】また、外部のパスポートサーバ50等とデータの送信を行うため、クライアント端末11には、送信手段27が設けられている。

【0089】なお、1つ目のタイプでは、サービスサイト40側の数分だけ、対応する公開鍵SS-AがROM18内部に記憶されている。すなわち、ROM18には、秘密鍵PC-Bは、夫々のクライアント端末11に特有なものが1つのみ記憶されていると共に、公開鍵SS-Aは、ユーザが予め登録しているサービスサイト40の分だけ記憶されている。

【0090】また、1つ目のタイプのクライアント端末11のワーク領域22は、特徴点抽出アルゴリズム24の起動、或いは生体情報照合アルゴリズム25の起動のための作業領域であり、RAM17内部に一定の領域が確保されているものである。以上のようなRAM17とROM18を備えたメモリ領域16が、インターフェース13に配置されて設けられている。

【0091】また、図2に示す2つ目のタイプは、生体情報を照合して特定人であるか否かの認証は行うが、パスポート情報はパスポートサーバ50側でないと得られない構成である。

【0092】この2つ目のタイプのメモリ領域16は、1つ目のタイプと異なってRAM17内にインターネットパスポート領域21が存在しない。代わりに、ROM18内にデポジットID30及びデポジットKey31が記憶されている。それ故、生体情報読取手段12で生体情報を読み取らせると、クライアント端末11側で特定人であるか否かの認証を行い、特定人であると認証されたときに、デポジットID30及びデポジットKey31を得る。それによって、パスポートサーバ50側での認証を必要としない構成である。

【0093】また、ROM18には、1つ目のタイプと同様に秘密鍵PC-Bが記憶されているが、1つ目のタイプとは異なって、サービスサイト40側の公開鍵SS-Aではなく、パスポートサーバ50側の公開鍵SV-Aが記憶されている。すなわち、2つ目のタイプでは、パスポートサーバ50側の公開鍵SV-Aを1つのみROM18に記憶している構成である。

【0094】なお、その他の部分は、上述の1つ目のメモリ領域16の構成と同様である。

【0095】さらに、図3に示す3つ目のタイプのメモリ領域16は、RAM17内にワーク領域22が初期状態で存するのみである。また、ROM18内には、生体情報照合アルゴリズム25が存せず、オペレーションソフトウェア23、特徴点抽出アルゴリズム24、秘密鍵PC-B、及び公開鍵SV-Aが格納されているのみである。すなわち、この構成では、生体情報照合アルゴリズム25がクライアント端末11側には記憶されていない。その代わり、パスポートサーバ50側にアクセスした状態で初めて生体情報の照合が行われる、いわばサーバ認証型の構成である。なお、RAM17に一度デポジットID30を入力すれば、以後このデポジットID30を記憶保存する、いわば識別情報記憶部を設けるように構成しても構わない。

【0096】なお、以下の説明では、1つ目のタイプから3つ目のタイプの夫々で、パスポートサーバ50側の構成が異なり、また作用も異なるため、夫々のタイプについて、説明することとする。また、以下の説明では、上述のクライアント端末11側の作用をまず説明し、続いてパスポートサーバ50側の構成の説明をすると共に、併せてパスポートサーバ50側の作用についても説明する。

【0097】(1つ目のタイプ) 図1及び図4に示す1つ目のタイプのクライアント端末認証型のクライアント端末11では、ユーザは、クライアント端末11の電源をオンにする。すると、まず初めにCPU15はオペレーションソフトウェア23を読み込み、活動を開始する状態となる。しかしながら、生体情報読取手段12の全ての行動は、インターフェース13を介してオペレーションソフトウェア23の上位アプリケーションの指示要求に基づいており、この生体情報読取手段12自らが行動を行うことはない。すなわち、CPU15は、常時、インターフェース13を監視している状態となる。

【0098】この状態で、図4に示すようにユーザがクライアント端末11を用いて特定のサービスサイト40にアクセスする。そして、このサービスサイト40でユーザが商品の購買を希望したり、情報コンテンツの閲覧やダウンロードを希望したとする。すると、このサービスサイト40側では、ユーザの認証を行う必要があるため、ユーザに対して認証要求をする。この場合、例えばサービスサイト40のWeb画面に、「認証ボタン」

等を表示させ、この認証ボタンをクリックする。

【0099】Web画面上の認証ボタンをクリックした場合、クライアント端末11は、認証実行状態となる。すなわち、CPU15は、例えばオペレーションソフトウェア23に対して認証を実行させる状態となる。この状態で、CPU15が生体情報読取手段12に対して「生体情報読取要求」を通知する。すると、CPU15は、ユーザに対し表示手段や音声を通じて生体情報読取手段12によって生体情報を読み取らせるように指示を出す。なお、このような指示の表示を行うLED、或いは音声を発するスピーカを別途設ける構成としても構わない。また、インターフェース13を通じて、上位アプリケーションに対しても同様の指示を行う。すなわち、例えばパソコンの画面表示や音声等の如きマンマシンインターフェース13を用いてユーザに生体情報の読み取り作業を行うよう、促すようにするものである。

【0100】ここで、例えば指紋の如き生体情報の表面にごみや汚れがついている場合、或いは例えば指紋読取スキャナにおいて、スキャナチップの表面が汚れていて一定基準の品質の指紋画像が採取できない場合がある。この場合は、一定基準の品質をクリアする画像が採取できるまで、指紋画像の読み取りを行う。

【0101】続いて、CPU15は生体情報読取手段12によって読み取られた生体情報を、RAM17のワーク領域22に一時的に格納する。そして、CPU15は、ワーク領域22に格納された生体情報をDSP14に送り込み、画像処理を要求する。この場合の画像処理とは、細線化や2値化等である。細線化とは、指紋の模様を均一な細い線に変換する画像処理のことである。また、2値化とは、生画像が例えば8階調コントラストであるとき、この8階調コントラストをある一定値のコントラスト値、例えば4等をしきい値として、それ以下は黒、それ以上を黒としてコントラストを2階調に分けてしまうことである。

【0102】細線化や2値化等の画像処理が終了したら、DSP14は修理後画像をRAM17のワーク領域22に格納する。そして、CPU15に対して画像処理終了を通知する。この通知を受け取ったCPU15は、特徴点抽出アルゴリズム24を起動させ、処理後の画像をこの特徴点抽出アルゴリズム24に手渡す。特徴点抽出アルゴリズム24は、生体情報の画像の特徴点の抽出を行った後に、特徴点データをRAM17のワーク領域22に保存し、処理の終了をCPU15に通知する。そして、特徴点抽出アルゴリズム24は、自動的に処理を終了する。

【0103】なお、例えば生体情報として指紋データを用いた場合には、特徴点抽出方法は、例えば日本電気株式会社が採用しているマニューシャ抽出方式等を用いることが好ましい。しかしながら、かかるマニューシャ抽出方式以外にも、種々の方式を採用しても何等問題はな

い。

【0104】特徴点抽出アルゴリズム24から処理終了通知を受け取ったCPU15は、生体情報照合アルゴリズム25を起動する。そして、CPU15は、生体情報照合アルゴリズム25に対して、「生体情報照合要求」を行う。その後、CPU15は、RAM17のワーク領域22に存在する特徴点データを生体情報照合アルゴリズム25に渡す。

【0105】CPU15から「生体情報照合要求」を受け取った生体情報照合アルゴリズム25は、ワーク領域22に存している特徴点データと、予めRAM17に存している生体情報特徴点データ20の照合処理を行う。その結果、ある一定のしきい値を下回っていれば、符合しなかったとしてその結果をCPU15に通知する。また、ある一定のしきい値を上回っていれば、符合したとしてその結果をCPU15に通知する。

【0106】ここで、生体情報が符合しなかった場合、CPU15は上位アプリケーションに対してインターフェース13を介し、「認証できませんでした」等の表示を行い、ユーザに対して通知する。逆に、生体情報が符合した場合、CPU15はインターネットパスポート領域21にアクセスする。そして、インターネットパスポート領域から、パスポート情報を取得可能となる。

【0107】なお、インターネットパスポート領域21の詳細については、後述する(2つ目のタイプ)のインターネットパスポートデータベース53の欄で説明する。通常、パスポート情報は、特定のサービスサイト40へアクセスするためのIDやパスポート、或いはクレジットカード会社等の決済機関のカード番号やパスポート等である。以下、これらをパスポート情報として説明する。

【0108】この場合、取得されたパスポート情報は、「認証ボタン」がクリックされた特定のサービスサイト40に、クライアント端末11から伝送される。なお、特定のサービスサイト40に対しては、特定のサービスサイト40のパスポート情報に、後述するように暗号化を施してから伝送を行う方式でも良く、また特定のサービスサイト40のパスポート情報に替えて、他の情報(例えば、認証OKサイン等)に暗号化を施してから伝送を行う方式としても良い。なお、以下の説明では、特定のサービスサイト40のパスポート情報に対して暗号化を施して伝送する場合について説明する。

【0109】クライアント端末11から特定のサービスサイト40のパスポート情報を該サービスサイト40側に伝送する場合、このパスポート情報に対してオペレーションソフトウェア23の有する暗号化処理機能によって暗号化処理が為される。すなわち、CPU15とオペレーションソフトウェア23、及び秘密鍵PC-B、公開鍵SS-Aによって暗号化手段が構成される。この暗号化処理では、特定のサービスサイト40のパスポート

情報（ID及びパスワード等）を原文とすると共に、もう1つ同じパスポート情報のコピーを生成する。

【0110】そして、このコピーをハッシュ関数によって圧縮して原文のダイジェスト版を作成する。その後、送信者はダイジェスト版に対して自分の秘密鍵PCBで暗号化する。それにより、ダイジェスト版がデジタル署名となる。さらに、このデジタル署名を原文に添付する。そして、原文及び添付されたデジタル署名の両方に対し、サービスサイト40側の公開鍵SSAで暗号化し、送信対象を秘匿化する。そして、その後SSL通信によってサービスサイト40サーバ側に原文及びデジタル署名を暗号化データとして送信する。

【0111】ここで、SSL (Secure Socket Layer) 通信とは、Netscape Communications社が開発した、インターネット上で情報を暗号化して送受信するプロトコルを用いて行う通信方式である。SSL通信では公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができるように為されている。OSI参照モデルではトランスポート層(第4層)に

あたり、HTTPやFTPなどの上位のプロトコルを利用するアプリケーションからは、特に意識することなく透過的に利用することができる。

【0112】サービスサイト40側で暗号化データを受信すると、まずサービスサイト40側の鍵情報記憶部41に記憶されている秘密鍵SSBによって復号化を行う。これは、公開鍵SSAによって暗号化された暗号化データを復号化し得るのは、サービスサイト40側が所持する秘密鍵SSBだからである。すると、サービスサイト40側では、原文であるパスポート情報を得ると共に、デジタル署名を得ることになる。続いて、サービスサイト40側では、同じく鍵情報記憶部41に記憶されている公開鍵PCAを用いてデジタル署名の検証を行う。そして、この検証によって、サービスサイト40側では、原文のダイジェスト版を得ることができる。

【0113】すなわち、クライアント端末11の秘密鍵PCBに対応した公開鍵PCAを用いて検証することができれば、秘密鍵PCBを所持しているクライアント端末11は、正当なクライアント端末11であるとみなされる。それによって、クライアント端末11の端末認証が、最初に行われる。なお、このような検証は、サービスサイト40側のサーバが有している復号化検証アルゴリズムによって為される。すなわち、ネットワークの途中で誰かが不正に暗号化データを入手し、これを改ざんした場合、改ざんされたデジタル署名によっては、ダイジェスト版が得られなく、それによって途中で改ざんされたか否かを検証することが可能となる。

【0114】上述の検証によって、正当なユーザであるとサービスサイト40側で判断された場合には、復号化されたパスポート情報に基づいて、最終認証を行う。す

なわち、パスポート情報がサービスサイト40で利用できるものであるか否かの確認を行う。その結果、ユーザが該サービスサイト40を利用できる者である、と判断された場合には、サービスサイト40側では、ユーザに対して「ログオン承認」の通知を行う。以上のようにして、1つ目のタイプにおけるユーザの認証が為される。

【0115】(2つ目のタイプ) 図2及び図5に示す2つ目のタイプのサーバ認証型のクライアント端末11では、基本的に、ユーザが生体情報を読み取らせて、生体情報の照合を行う部分までは同じである。そして、この生体情報の照合を行ってから後の部分がやや異なるものとなっている。

【0116】生体情報が符合した場合、CPU15はROM18に格納されているデポジットKey31を、上述の1つ目のタイプで述べたような、自らの生体情報読取手段12に対して発行されている公開鍵暗号インフラ方式を用いて暗号化する。なお、1つ目のタイプと異な

って、2つ目のタイプではROM18にパスポートサーバ50側の公開鍵SV-Aが記憶されている。このため、デジタル署名及び原文は、公開鍵SV-Aで暗号化されることとなる。

【0117】なお、2つ目のタイプでは、暗号化データと共に、サービスサイト40のURL情報も一緒に伝送する。このURL情報は、暗号化されても暗号化されなくても構わない。

【0118】SSL通信によってパスポートサーバ50側に原文及びデジタル署名がクライアント端末11から暗号化データとして送信され、パスポートサーバ50側のアクセス手段51でこの暗号化データを受信する。すると、上述の1つ目のタイプで述べたのと同じような暗号化データの復号化・検証が行われる。この場合、1つ目のタイプと異な

って、復号化はパスポートサーバ50の鍵情報記憶部52に記憶されている秘密鍵SV-Bと公開鍵PCAによって為される。また、この暗号化データの復号化・検証によって得られるのは、デポジットID30及びデポジットKey31である。

【0119】なお、鍵情報記憶部52には、後述する公開鍵SS-Aも別途記憶されている。

【0120】パスポートサーバ50側での復号化・検証により、正当なユーザであると判断された場合には、復号化されたデポジットID30及びデポジットKey31に基づいて、パスポートサーバ50が有しているインターネットパスポートデータベース53の検索を行う。この検索は、インターネットパスポートデータベース53に、復号化されたデポジットID30及びデポジットKey31に対応するWebデポジット54が存在するか否かの検索である。

【0121】なお、インターネットパスポートデータベース53は、上述の1つ目のタイプにおけるインターネットパスポート領域21が、各個人毎に複数存在して設

けられている。この場合、各個人毎のクライアント端末11におけるインターネットパスポート領域21は、Webを介したメモリ空間上に存在するので、各個人毎のWebデポジット54となっている。そして、このWebデポジット54がパスポート情報記憶手段としての機能を果たしている。

【0122】その結果、対応するWebデポジット54が存在する場合には、このWebデポジット54から対応するサービスサイト40のパスポート情報を得る。この場合、Webデポジット54から対応するサービスサイト40のパスポート情報を得るために、URL情報に基づいてWebデポジット54内の検索を行う。

【0123】ここで、パスポートサーバ50に存するWebデポジット54内のデータの構成について、例示で示した図7に基づいて説明する。この図に示すパスポート情報には、ユーザのアクセス権利によって、以下のレベルに分類されている。この図に示すように、ユーザのアクセス権利の分類は、＜書込み許可権利・削除権利＞、＜存在を知ることができる＞、＜内容を見ることができる＞、＜書換えできる＞、＜ワンタイム書込みができる＞、＜利用できる＞となっている。

【0124】また、ユーザのパスポート情報には、例えば、「デポジットID」、「第三者機関記載情報」、「サービスサイト記載情報」、「公的機関記載情報」、「民間企業記載情報」、「ユーザ記載情報」、「生体情報」、「アルゴリズム」がある。

【0125】これらのパスポート情報のアクセスレベルは、例えばフラグの設定によって行う。すなわち、例えばデポジットID30専用のフォルダを作成し、このフォルダのプロパティ中のフラグの設定を行うことにより為される。例示したデポジットID30へのアクセス権利では、＜書込み許可権利・削除権利＞という権利はないので、これに対応したフラグを「0」に設定する。また、＜存在を知ることができる＞という権利はあるので、これに対応したフラグを「1」に設定する。

【0126】また、別のアクセスレベルの分類としては、全てのアクセス権利を有する、フルアクセス可能な状態を数字の「0」で表し、以下、アクセス権利が制限されるに従って、大きな数字を割り振ることにより行うものがある。この場合では、＜書込み許可権利・削除権利＞～＜利用できる＞までの行と、「デポジットID」～「アルゴリズム」までの列における組み合わせの分だけ数字を割り振り、その数字にアクセス権利を対応させる。このようにしても、アクセス権利の制御が実現可能となる。

【0127】なお、「決済機関情報」や、「サービスサイト情報」等は、複数の決済機関情報や複数のサービスサイト情報が記載されているため、複数の情報を保存しておくフォルダを形成し、このフォルダ毎にフラグの設定を行うように構成しても構わない。

【0128】以上の如く、ユーザのアクセス権利の分類がなされたものの例示としては、「○」ができる、「×」ができない、「△」がサービスサイト40の方針でできたりできなかったりする、で示す。この場合、「デポジットID」は、＜書込み許可権利・削除権利＞は×、＜存在を知ることができる＞は○、＜内容を見ることができる＞は○、＜書換えできる＞は×、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。また、「第三者機関記載情報」、「決済機関情報」、「サービスサイト記載情報」、「公的機関記載情報」、及び「民間企業記載情報」は、＜書込み許可権利・削除権利＞は○、＜存在を知ることができる＞は○、＜内容を見ることができる＞は△、＜書換えできる＞は×、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。

【0129】さらに、「ユーザ記載情報」は、＜書込み許可権利・削除権利＞は○、＜存在を知ることができる＞は○、＜内容を見ることができる＞は○、＜書換えできる＞は○、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。また、「生体情報」は、＜書込み許可権利・削除権利＞は×、＜存在を知ることができる＞は○、＜内容を見ることができる＞は×、＜書換えできる＞は×、＜ワンタイム書込みができる＞は○、＜利用できる＞は○となっている。また、「アルゴリズム」は、＜書込み許可権利・削除権利＞は×、＜存在を知ることができる＞は○、＜内容を見ることができる＞は×、＜書換えできる＞は×、＜ワンタイム書込みができる＞は×、＜利用できる＞は○となっている。

【0130】しかしながら、アクセス権利の設定は、上述のものには限られず、インターネットパスポートデータベース53の管理者は、パスポート情報の重要性に鑑みて種々設定可能である。

【0131】このような構成のデポジット領域から、必要なパスポート情報がパスポートサーバ50に引き出されると、このパスポート情報に基づいて、パスポートサーバ50はアクセス手段51を介してログオン要求が為されている特定のサービスサイト40のサーバにアクセスする。なお、特定のサービスサイト40へのログオンは、パスポート情報と共に伝送されてきたURLに基づいて行う。

【0132】この場合、パスポート情報がパスポートサーバ50に引き出されると、このパスポート情報に基づいて、特定のサービスサイト40にログオン要求が為される。この場合、特定のサービスサイト40に対してパスポート情報を伝送することになるが、該特定のサービスサイト40へのパスポート情報の伝送に際しては、パスポート情報に対して暗号化を施して伝送する。

【0133】すなわち、上述の1つ目のタイプで説明したクライアント端末11での暗号化手段による暗号化処理と同様に、パスポート情報を原文とすると共に、もう

1つの同じパスポート情報のコピーを生成する。そして、このコピーをハッシュ関数によって圧縮して原文のダイジェスト版を作成する。その後、送信者はダイジェスト版に対してパスポートサーバ50側の秘密鍵SV-Bで暗号化する。それにより、ダイジェスト版がデジタル署名となる。さらに、このデジタル署名を原文に添付する。そして、原文及び添付されたデジタル署名に対し、サービスサイト40側の公開鍵SS-Aで、原文とそれに添付したデジタル署名の両方を暗号化し、送信対象を秘匿化する。そして、その後にSSL通信によって

サービスサイト40側に原文及びデジタル署名を暗号化データとして送信する。
【0134】サービスサイト40側で暗号化データを受信すると、まずサービスサイト40側の鍵情報記憶部41に存している秘密鍵SS-Bによって復号化を行う。これは、公開鍵SS-Aによって暗号化された暗号化データを復号化し得るのは、パスポートサーバ50が所持する秘密鍵SS-Bだからである。すると、パスポートサーバ50側では、原文であるパスポート情報を得ると共に、デジタル署名を得ることになる。続いて、サービス

サイト40側では、鍵情報記憶部41に存している公開鍵SV-Aを用いてデジタル署名の検証を行う。そして、この検証によって、パスポートサーバ50側では、原文のダイジェスト版を得ることができる。
【0135】このように、パスポートサーバ50の秘密鍵SV-Bに対応した公開鍵SV-Aを用いて検証することができれば、秘密鍵SV-Bを所持しているパスポートサーバ50は、正当なものである、とみなされる。それによって、パスポートサーバ50の端末認証が、最初に為される。なお、このような検証は、パスポートサーバ50が有している復号化検証アルゴリズムによって

為される。すなわち、ネットワークの途中で誰かが不正に暗号化データを入手し、これを改ざんした場合、改ざんされたデジタル署名によっては、ダイジェスト版が得られなく、それによって途中で改ざんされたか否かを検証することが可能となる。
【0136】上述の検証によって、パスポートサーバ50が正当なものであるとサービスサイト40側で判断された場合には、復号化されたパスポート情報に基づいて、最終認証を行う。すなわち、パスポート情報がサービスサイト40で利用できるものであるか否かの確認を行う。その結果、ユーザが該サービスサイト40を利用できる者である、と判断された場合には、サービスサイト40側では、ユーザに対して「ログオン承認」の通知を行う。以上のようにして、2つ目のタイプにおけるユーザの認証が為される。

【0137】(3つ目のタイプ) 3つ目のタイプのサーバ認証型では、クライアント端末11側で生体情報の照合を行わないものである。この3つ目のタイプでは、1つ目のパターン及び2つ目のパターンで述べた特徴点抽

出アルゴリズム24によって生体情報の特徴点抽出を行う部分までは、同じである。そして、ここから後の部分がやや異なるものとなっている。

【0138】特徴点抽出アルゴリズム24によって生体情報の特徴点を抽出し、この終了通知をCPU15が受け取った後に、RAM17のワーク領域22に存在する特徴点データを自らのクライアント端末11(生体情報読取手段12)に対して発行されている秘密鍵PC-Bで暗号化する。この場合、特徴点データのみならず、クライアント端末11がデポジットID30を記憶している場合には、このデポジットID30も一緒に秘密鍵PC-Bで暗号化する。

【0139】なお、以下の暗号化の手順は、上述の2つ目のタイプで述べたデポジットID30及びデポジットKey31の暗号化の手順と同じである。すなわち、原文を特徴点が抽出された生体情報(特徴点データ)及びデポジットID30とし、この原文に対してコピーを作成する。そして、このコピーをハッシュ関数によって圧縮して原文のダイジェスト版を作成する。その後、このダイジェスト版をクライアント端末11側の秘密鍵PC-Bで暗号化してデジタル署名を作成する。

【0140】そして、このデジタル署名を原文に添付し、原文及び添付されたデジタル署名の両方をパスポートサーバ50側の公開鍵SV-Aで暗号化して全体の秘匿化を図る。そして、この後にSSL通信によってパスポートサーバ50側に原文及びデジタル署名を暗号化データとして送信する。

【0141】なお、3つ目のタイプでも、暗号化データと共にサービスサイト40のURL情報と一緒に伝送する。このURL情報は、暗号化されても暗号化されなくても構わない。

【0142】パスポートサーバ50側のアクセス手段51で暗号化データを受信すると、まずパスポートサーバ50側の鍵情報記憶部52に存している秘密鍵SV-Bで復号化を行う。すると、パスポートサーバ50側では、原文である生体情報(特徴点データ)及びデポジットIDを得ると共に、デジタル署名を得ることとなる。続いて、パスポートサーバ50側では、鍵情報記憶部52の公開鍵PC-Aを用いてデジタル署名の検証を行う。そして、この検証によって、パスポートサーバ50側では、原文のダイジェスト版を得ることができる。このダイジェスト版が得られるか否かで、デジタル署名が改ざんされたか否かを検証することが可能となる。

【0143】ここで、パスポートサーバ50内には、照合用の生体情報が生体情報データベース55に登録されている。この生体情報データベース55は、上述の1つ目のタイプ及び2つ目のタイプにおける生体情報特徴点データ20に対応するものである。かかる生体情報データベース55は、各個人毎の生体情報特徴点データ20を、多人数分登録しているものである。

10

20

30

40

50

【0144】また、生体情報データベース55には、生体情報照合手段56が接続されている。生体情報照合手段56は、上述の1つ目のタイプ及び1つ目のタイプにおけるのと同様な生体情報照合アルゴリズム57を有するものである。なお、3つ目のタイプにおいては、かかる生体情報アルゴリズム57と共に、生体情報データベース55から引き出された照合用の生体情報特徴点データ20を引き出して作業するためのメモリ空間58も有する構成である。

【0145】生体情報での認証を行う場合には、復号された生体情報（特徴点データ）と、生体情報データベース55から照合用の生体情報特徴点データ20とを生体情報照合手段56のメモリ空間58に引き出す。そして、生体情報照合アルゴリズム57にてこれら両生体情報の照合を行う。

【0146】この照合の結果、両生体情報が符合すると判断された場合、生体情報照合手段56から「OK」のサインがアクセス手段51に出される。このアクセス手段51が「OK」のサインを受け取った場合、アクセス手段51からインターネットパスポートデータベース53にパスポート表示命令が出される。なお、インターネットパスポートデータベース53の構成は、上述の1つ目のパターンで述べたのと同様である。

【0147】また、インターネットパスポートデータベース53からアクセス手段51にパスポート情報が引き出され、特定のサービスサイト40にログオン要求する場合も、上述の2つ目のタイプと同様である。

【0148】このように、3つ目のタイプは、生体情報を2つ目のタイプにおけるデポジットKey31に見立て、デポジットID30及びデポジットKey30に対応するWebデポジット54を検索し、このWebデポジット54から目的とするパスポート情報を得るものである。

【0149】なお、3つ目のタイプでは、生体情報データベース54と生体情報照合手段56を、パスポートサーバ50から分離して、別途認証サーバに設ける構成としても構わない。パスポートサーバ50と別途の認証サーバを設ける場合には、これらパスポートサーバ50と認証サーバの間がネットワーク回線によって接続されている。

【0150】このような構成の認証システム10、認証方法によると、1つ目のタイプから3つ目のタイプまで、共に生体情報を生体情報読取手段12で読み取り、特定人の生体情報と符合させる。そして、生体情報が符合すれば、Webデポジット54に記憶されているパスポート情報を引き出して、パスポートアクセス手段によってこのパスポート情報に対応したサービスサイト40にアクセスする。このため、生体情報の読み取りのみによって所定のサービスサイト40にアクセス可能となり、複数のサービスサイト40のIDやパスワードに対

応させることができる。

【0151】このようにしたことで、一々複数のIDやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイト40の認証を行うことが可能となる。また、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイト40での認証を行うことが可能となる。

【0152】また、読取生体情報記憶部と照合回避手段を設けた場合には、一度読み取られた生体情報を読取生体情報記憶部に記憶させておき、この読取生体情報記憶部に記憶されている生体情報と同一の生体情報に基づく照合を、照合回避手段で拒否することができる。すなわち、他人が不正に特定人の生体情報を入手した場合、その生体情報を用いて生体情報の照合を行おうとしても、読取生体情報記憶部に記憶されている生体情報を用いることはできない。これは、例えば指紋のような生体情報では、押圧角度や押圧面積、或いは押圧力が同じである全く同一の生体情報が得られることはほとんどないことに基づくものである。

【0153】このような読取生体情報記憶部、及び照合回避手段をパスポートサーバ50内に設けた場合には、パスポートサーバ50内に一度照合した生体情報を蓄えておくことができる。そして、蓄えられた生体情報と同一の生体情報がパスポートサーバ50に送信されてきた場合には、照合回避手段で生体情報の照合を回避することが可能となる。すなわち、2つ目のタイプ及び3つ目のタイプに適したものとなる。

【0154】また、読取生体情報記憶部、及び照合回避手段をクライアント端末11内に設けた場合には、クライアント端末11側で一度照合した生体情報を蓄えておくことができ、この蓄えられた生体情報と同一の生体情報が生体情報読取手段12で読み取られた場合には、照合回避手段で生体情報の照合を回避することが可能となる。

【0155】また、1つ目のタイプでは、クライアント端末11に生体情報特徴点データと、生体情報照合アルゴリズム25と、インターネットパスポート領域21と、を有している。そのため、クライアント端末11側で特定人か否かの認証が行え、この認証に基づいてインターネットパスポート領域21からパスポート情報を取得し、このパスポート情報に基づいて特定のサービスサイト40にアクセス可能となる。

【0156】また、2つ目のタイプでは、クライアント端末11に生体情報特徴点データと、生体情報照合アルゴリズム25と、を有している。このようにすることで、クライアント端末11側で特定人か否かの認証が行え、この認証に基づいてデポジットKey31を取得し、デポジットID30及びデポジットKey31に基づいてインターネットを介してインターネットパスポート

トデータベース53にアクセスすることができる。

【0157】また、3つ目のタイプでは、クライアント端末11で特定人か否かの認証は行わずに、パスポートサーバ50側で特定人か否かの認証を行い、この認証に基づいてインターネットパスポートデータベース53にアクセスするものである。このようにすることで、完全にパスポートサーバ50側で認証を行う構成となる。すなわち、1つ目のタイプ及び2つ目のタイプと異なっ

て、3つ目のタイプでは、クライアント端末11を交換しても、特定人か否かの認証を行うことが可能となる。

【0158】また、3つ目のタイプにおいては、生体情報照合手段とインターネットパスポートデータベース53とが同一のパスポートサーバ50内に設けられている。このため、生体情報を照合してインターネットパスポートデータベース53からパスポート情報を引き出す場合、パスポート情報の引き出しまでの時間の短縮化を図ることが可能となる。

【0159】また、3つ目のタイプでは、クライアント端末11単独で生体情報の読み取りを行い、読み取られた生体情報をパスポートサーバ50に伝送するものである。このため、ユーザが所持可能なクライアント端末11を用いて簡易に生体情報を読み取らせ、読み取らせた生体情報とパスポート情報を対応させることで、生体情報をサービスサイト40に対する身分証明手段として、シングルサイン感覚で簡易に用いることが可能となる。

【0160】また、クライアント端末11は、DSP14、特徴点抽出アルゴリズム24、鍵情報記憶部26及び暗号化手段としてのオペレーションソフトウェア23、秘密鍵PC-B、公開鍵SV-A（公開鍵S-A）を有している。このため、DSP14でデータ処理が為され、特徴点抽出アルゴリズム24で特徴点の抽出が為された生体情報に対して秘密鍵PC-Bで暗号化した後に公開鍵SV-A（公開鍵S-A）で暗号化を行う。このようにしてからパスポートサーバ50に伝送すれば、例えば伝送経路の途中で他人が不正に生体情報を入力しても、解読が極めて困難なものとなり、生体情報の伝送に際しての安全性を確保することが可能となる。

【0161】また、クライアント端末11独自の秘密鍵PC-Bで暗号化した後に、パスポートサーバ50側の公開鍵SV-A（公開鍵S-A）で暗号化するので、伝送経路の途中で他人が不正に生体情報を入力し、入手した生体情報に基づいて改ざんを加えて他人が特定人に成りすまそうとしても、逆関数のないハッシュ関数の性質から、改ざんしたか否かを容易に検知することが可能となる。すなわち、事実上、特定人に成りすますることが不可能となる。

【0162】さらに、2つ目のタイプ及び3つ目のタイプでは、生体情報が生体情報データベース54に登録されるに際してデポジットID30が割り当てられている。このため、生体情報照合手段56での生体情報の照

合を行うに先立って、このデポジットID30に基づいて生体情報データベース54に登録されている生体情報特徴点データ20を特定することが可能となる。すなわち、かかるデポジットID30に基づいて生体情報の検索を行うことにより、生体情報の照合の時間の短縮化を図ることができる。

【0163】また、かかるデポジットID30をクライアント端末11に記憶させることにより、クライアント端末11側で生体情報の読み取りを行って伝送する場合、一々特定人がデポジットID30を入力しなくても済む。なお、このデポジットID30も暗号化すれば、デポジットID30の秘匿化を図ることができ、このデポジットID30の解読が極めて困難となって安全性を確保することができる。

【0164】さらに、Webデポジット54は、アクセスレベル別に分類されている。ここで、パスポート情報は、生体情報と対応するように設けられているので、生体情報読取手段12によって生体情報を読み取らせると、この生体情報に対応したパスポート情報を引き出すことができる。この場合、IDやパスワードの如き単なる情報ではなく、生体情報を自己の身分証明手段として用いて認証を行うため、他人が特定人に成りすますのを防止することができる。

【0165】さらにユーザのアクセスレベルの設定により、ネットを介しての会員制サービスサイト、或いは決済機関、公的機関、民間企業等が運営する、種々のサービスサイトにメリットが生ずることとなる。例えば、決済機関の情報を記載している場合、ユーザのアクセスレベルを「存在を知ることができる」を○として、「書換えできる」を×とした場合、ユーザは勝手にパスポート情報であるIDやパスワードを書き換えることができない。このようなアクセスレベルの設定により、各サイト側において生体情報を活用した本人の絶対認証を現実的に利用可能となる。

【0166】また、例えばデータを保存する領域をWebデポジット54内に設けた場合、アクセスレベルの設定の仕方によってはデータの保存はできるがコピーはできないようにすることもできる。この場合には、特定人は生体情報を用いてアクセス可能となり、Webデポジット54内でそのデータをアクセスレベルに設定されたレベル内で利用可能となるが、違法なコピー等は行えないものとなる。それによって、種々のコンテンツからデータを該Webデポジット54内にダウンロードした場合、他の領域にはコピーできないため、該データの著作権を守ることが可能となる。

【0167】また、Webデポジット54のアクセスレベルは、パスポート情報に関するデータの書込みや削除を行えるレベルと、パスポート情報に関するデータの存在を知ることができるレベルと、パスポート情報に関するデータの内容を見ることができるレベルと、パスポート

ト情報に関するデータの書換えが行えるレベルと、パスポート情報に関するデータのワンタイムの書込みができるレベルと、パスポート情報に関するデータの利用ができるレベルに分類されている。

【0168】このように各レベルに分けて分類したことにより、夫々のサービスサイト40が要求する状態に、ユーザのアクセス権利を制限することが可能となる。これによって、生体情報の読み取りで該Webデポジット54にアクセスした場合、ユーザに対してもIDやパスワードの秘匿性を確保することも可能となる。

【0169】さらに、アクセスレベルの設定は、フラグの設定によってアクセスレベルを種々設定するので、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにWebデポジット54を設定できる。

【0170】なお、アクセスレベルの設定は、アクセスレベル別に割り当てられた数字の設定によって行うこともできる。このようにアクセスレベル別に割り当てられた数字の設定によってアクセスレベルを種々設定する場合も、簡易な操作でサービスサイト側の希望に沿ったアクセスレベルにWebデポジット54を設定することができる。

【0171】また、Webデポジット54には、パスポート情報に対応したサービスサイト40のURLも記憶されておくこともできる。この場合、生体情報データベース55に登録された生体情報と、生体情報読取手段12によって読み取られた生体情報とが符合した場合に、Webデポジット54から対応するパスポート情報と共にサービスサイト40のURLを引き出して、このURLに基づいてアクセス手段51で特定のサービスサイト40にアクセスすることが可能となる。すなわち、一々URLを検索したり入力せずに、特定のサービスサイト40にアクセス可能となる。

【0172】さらに、生体情報読取手段12には、読み取られた生体情報が基準の品質以下の場合に再度生体情報の読み取りを行うようにする生体情報判別手段を設けるようにしても良い。このように構成した場合には、基準の品質以上の生体情報にて特定人か否かの認証を行える。それによって、例えば生体情報読取手段の汚れによって一定基準以下の生体情報に基づく認証を行うのを防止することができ、認証精度の向上を図ることができる。

【0173】以上、本発明の一実施の形態について説明したが、本発明はこれ以外にも種々変形可能である。以下、それについて説明する。上述の実施の形態では、デジタル署名を秘密鍵PC-Bで暗号化し、このデジタル署名と原文とを公開鍵S-A(SV-A)で暗号化してからSSL通信で送信している。しかしながら、デジタル署名を生成せずに、単に原文を秘密鍵PC-Bで暗号化した後に、公開鍵S-A(SV-A)で暗号化してからSSL通信で送信するように構成しても構わな

い。

【0174】また、図6では、生体情報特徴点データ20は、Webデポジット54とは別個に設けられた生体情報データベース55に登録されているが、生体情報特徴点データ20を各個人毎のWebデポジット54内に登録させる構成としても構わない。このように、生体情報特徴点データ20をWebデポジット54内に登録する構成とした場合は、Webデポジット54の構成を示す図7の「生体情報」の欄に登録することとなる。

10 【0175】また、Webデポジット54に「生体情報」の欄を設けた場合、生体情報照合手段56をインターネットデータベース53内に設けるようにしても良い。この場合、インターネットデータベース53は、サーバ的な機能を果たすことになり、インターネットデータベース53とアクセス手段51との間で直接やり取りする構成となる。

【0176】また、「生体情報」をWebデポジット54内に設けると共に、生体情報アルゴリズム57を各個人毎のWebデポジット54内に設ける構成としても構わない。この場合、生体情報の照合は、全てWebデポジット54内で行える構成となり、セキュリティが向上する構成となる。この構成を採用する場合、Webデポジット54内の「アルゴリズム」の欄に生体情報アルゴリズムを記憶させておく。

【0177】

【発明の効果】本発明によれば、生体情報を生体情報読取手段で読み取り、特定人の生体情報と符合すれば、パスポート情報記憶手段に記憶されているパスポート情報を引き出して、アクセス手段によってこのパスポート情報に対応したサービスサイトにアクセスすることが可能となる。すなわち、生体情報の読み取りのみによって所定のサービスサイトにアクセス可能となり、複数のサービスサイトのIDやパスワードに対応させることができる。このため、一々複数のIDやパスワードを覚える必要がなく、利便性を向上させることが可能となる。すなわち、生体情報をシングルサイン感覚で読み取らせ、それに基づいた種々のサービスサイトの認証を行うことが可能となる。すなわち、ユーザは生体情報を自己の身分証明手段として用いるのみで、各サービスサイトでの認証を行うことが可能となる。

【図面の簡単な説明】

【図1】本発明の認証システムにおけるクライアント端末のうち、1つ目のタイプの構成を示す図である。

【図2】本発明の認証システムにおけるクライアント端末のうち、2つ目のタイプの構成を示す図である。

【図3】本発明の認証システムにおけるクライアント端末のうち、3つ目のタイプの構成を示す図である。

【図4】図1のクライアント端末を用いた認証システムの構成を示す図である。

【図5】図2のクライアント端末を用いた認証システム

37

の構成を示す図である。

【図6】図3のクライアント端末を用いた認証システムの構成を示す図である。

【図7】図1のクライアント端末のインターネットパスポート領域、又は図2若しくは図3の認証システムにおけるWebデポジットの構成を示す図である。

【図8】従来のリアル世界、準バーチャル世界、及びバーチャル世界における認証の差異を示す図である。

【符号の説明】

10…認証システム
11…クライアント端末（情報端末）
12…生体情報読取手段
14…DSP（データ処理手段）
15…CPU
17…RAM
18…ROM
20…生体情報特徴点データ（生体情報登録手段）

21…インターネットパスポート領域（パスポート情報記憶手段）

23…オペレーションソフトウェア

24…特徴点抽出アルゴリズム

25…生体情報照合アルゴリズム（生体情報照合手段）

26…鍵情報記憶部

27、41、52…送信手段

30…デポジットID

31…デポジットKey

10 40…サービスサイト

50…パスポートサーバ

51…アクセス手段

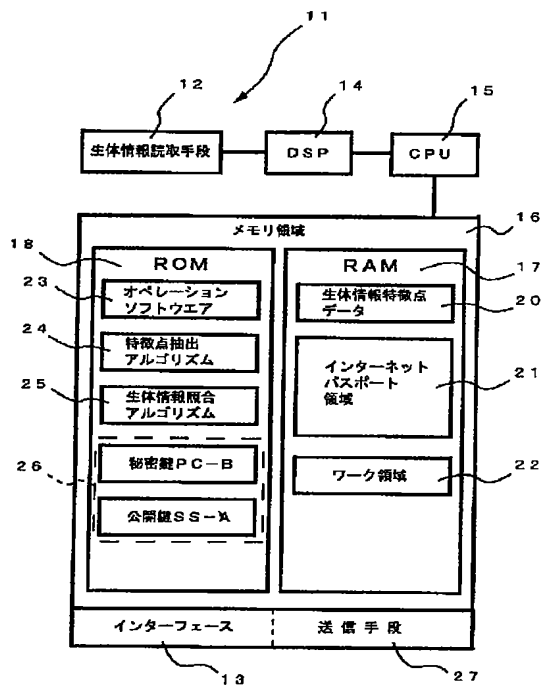
53…インターネットパスポートデータベース

54…Webデポジット

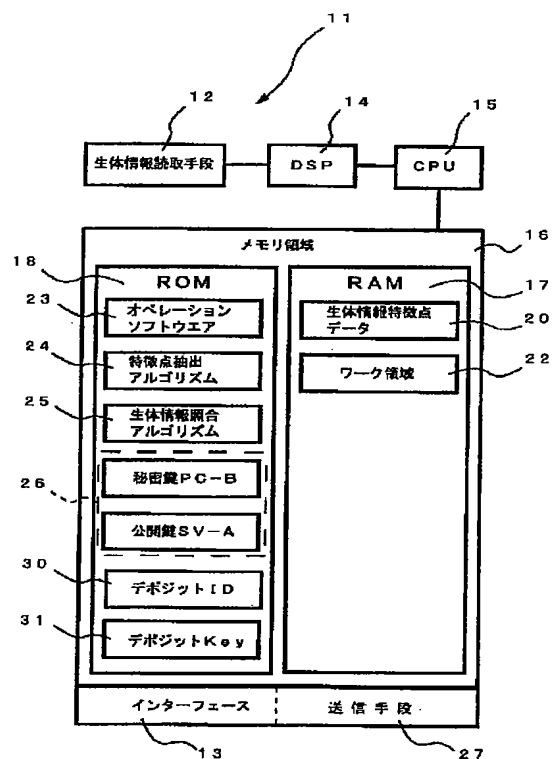
55…生体情報データベース（生体情報登録手段）

56…生体情報照合手段

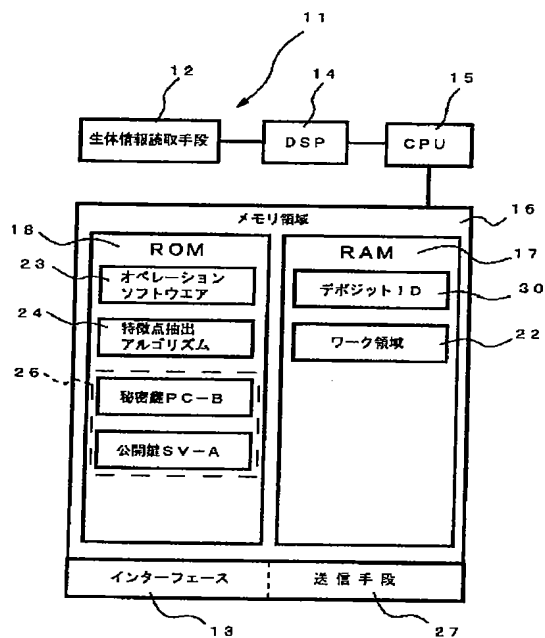
【図1】



【図2】



【図3】



【図7】

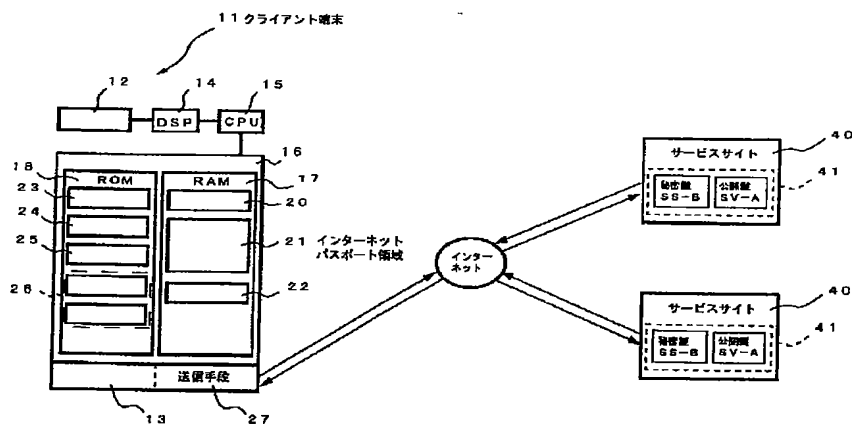
Webデポジット54の構成

ユーザーのアクセス権利

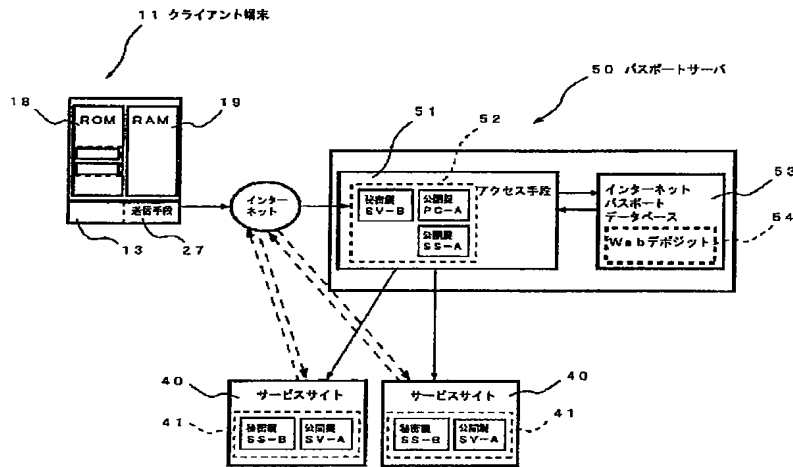
	書き込み許可 権利・ 削除権利	存在を知 ることがで きる	内容を見 ることがで きる	書き換えで きる	ワンタイ ム書き込み ができる	利用出来 る
Deposit ID	×	○	○	×	×	○
第三金 種預記 帳情報	○	○	△	×	×	○
決済機 関口座 情報	○	○	△	×	×	○
サービス サイト記 帳情報	○	○	△	×	×	○
公約機 関口座 情報	○	○	△	×	×	○
民衆企 業記帳 情報	○	○	△	×	×	○
ユーザー 記帳情 報	○	○	○	○	×	○
生 体 情 報	×	○	×	×	○	○
アルゴ リズム	×	○	×	×	×	○

○:出来る ×:出来ない △:サービスサイトの方針で出来たり出来なかったりする。

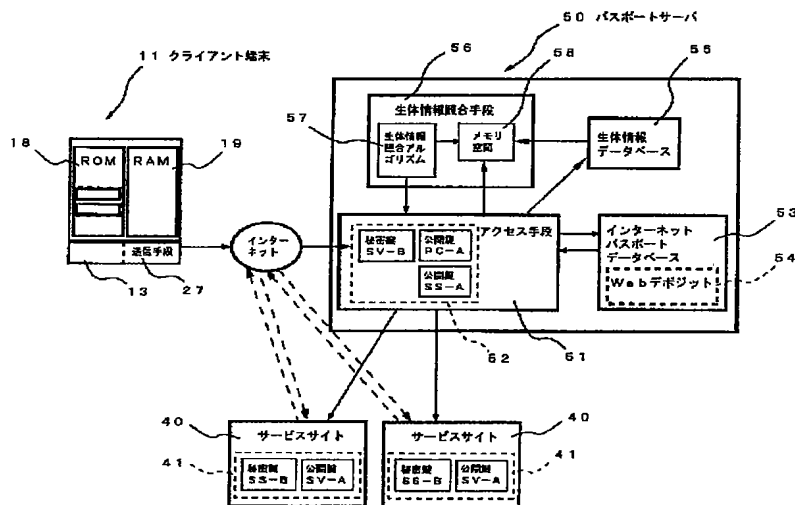
【図4】



【図5】



【図6】



【図8】

	リアル世界	準バーチャル世界	バーチャル世界
ハードウェアトークンの所有認証	○	○	×
ハードウェアトークンが偽造されていないか？	△	△	×
記憶トークンの記憶認証	○	○	○
記憶トークンが盗まれていないか？	×	×	×
顔認証	○	×	×
筆跡認証	○	×	×
監視カメラ撮影(防犯・バックアップ)	○	○	×

フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	ターム (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D
			6 7 5 D

F ターム (参考) 5B049 BB11 EE05 EE08 GG10
5B055 EE17 HA12 HB04
5B085 AE08 AE25
5J104 AA07 AA09 AA16 EA04 JA21
KA01 KA17 LA03 LA05 LA06
MA01 NA02 NA12 NA36 NA37
NA38 NA42

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-055959

(43)Date of publication of application : 20.02.2002

(51)Int.Cl.

G06F 15/00 G06F 17/60

G09C 1/00 H04L 9/32

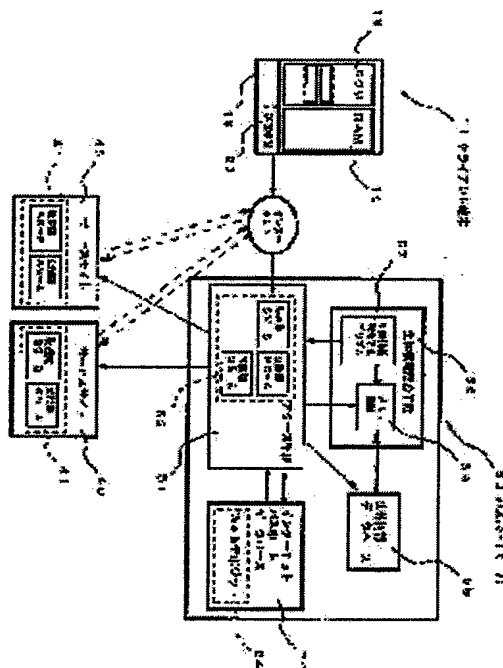
(21)Application number : 2000-243787

(71)Applicant : MACKPORT BIO-SECURITY CORP

(22)Date of filing : 11.08.2000

(72)Inventor : NAKANO YUJI

(54) INFORMATION TERMINAL AND SYSTEM AND METHOD FOR AUTHENTICATION



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system and a method for authentication with high security which makes it possible to easily and absolutely authenticate a specific person only with a single sign using living body information and disables others to illegally use the living body information.

SOLUTION: This authentication system 10 which manages information regarding the specific person through a network and authenticates whether or not a person accessing the information is the specific person is equipped with a living body information read means 12 which reads the living body information, a living body information registering means 55 which registers the living body information on the specific person for matching, a living body information matching means 56 which matches the pieces of living body information read by the living

body information registering means 55 and living body information read means 12 with each other, a passport information storage means 54 which stores pieces of passport information of respective service sites 40 so that they correspond to pieces of living body information registered in the living body information registering means, and an access means 51 which takes corresponding passport information out of the passport information storage means 54 when the pieces of living body information match each other and access the corresponding service site 40.